

This space is for the Federal Privacy Council. Users will only see collaborations to which they have specifically been given access by the collaboration owner.



PRIVACY COUNCIL

Search

[Council Home](#) [Full Council](#) [Committees](#) [Training and Resources](#) [FPC.gov](#)

Privacy Training

Privacy Resources

Federal Privacy Boot Camp

Welcome to the Spring 2022 Federal Privacy Boot Camp! If you have questions, please contact privacy.council@gsa.gov.

The Privacy Boot Camp is an 8-week program designed to provide foundational knowledge of Federal privacy laws and policies to staff who are new to privacy roles. It serves as a central standardized training resource for the Executive Branch. Attendees join a collaborative interagency network of professionals seeking to address complex issues in privacy that affect the Federal Government. This program is held in the spring and fall of each year, offered free of charge by the Federal Privacy Council, and open to Executive Branch employees.

- To subscribe to the general FPC listserv, please email privacy.council@gsa.gov.
- The program is currently only open to Federal employees.
- The program is limited to 60 participants.
- Materials from the Fall 2019 Privacy Boot Camp are available [here](#).
- Agendas and slide decks will be uploaded over the course of the Spring 2021 session.

Spring 2022 Federal Privacy Boot Camp

Agenda & Materials

Session 1 - Basic Privacy Overview

- [Agenda](#)
- [Slide Deck #1](#)
- [Slide Deck #2](#)

Session 2 - The Privacy Act

- [Agenda](#)
- [Slide Deck](#)

Session 3 - PIAs, FIPPs, Reporting

- [Agenda](#)
- [Slide Deck](#)

Session 4 - A-130

- [Agenda](#)
- [Slide Deck](#)

Session 5 - Privacy Breaches & Identity Theft

- [Agenda](#)
- [Slide Deck \(Identity Theft\)](#)
- [Slide Deck \(Privacy Breaches\)](#)

Session 6 - IT Security

- [Agenda](#)
- [Slide Deck \(IT Security\)](#)
- [Slide Deck \(RPA\)](#)

Session 7 - Contracts and Web Policies

- [Agenda](#)
- [Slide Deck \(Contracts\)](#)
- [Slide Deck \(Web Policies\)](#)

Session 8 - Other Privacy Laws

- [Agenda](#)
- [Slide Deck \(FTC\)](#)
- [Slide Deck \(HIPAA\)](#)
- [Slide Deck \(IC Panel\)](#)

Schedule

All sessions will be held online from 1:00pm to 5:00pm EST

- March 18, 2022 - Basic Privacy Overview
- March 25, 2022 - Privacy Act of 1974
- April 1, 2022 - PIAs and FIPPs
- April 8, 2022 - Circular A-130
- April 22, 2022 - Privacy Breaches
- April 29, 2022 - IT Security for Privacy Professionals
- May 6, 2022 - Contracts & Web Policies
- May 13, 2022 - Other Privacy Laws

[More](#)

Federal Privacy Boot Camp

Spring 2022 Agenda Session 1: Basic Privacy Overview

Title Session 1: Basic Privacy Overview

Date March 18, 2022 (Friday)

Location Virtual

Time 1:00 PM - 5:00 PM

Time	Topic	Presenter(s)
1:00 PM – 2:10 PM	History and Background on Privacy	(b) (7)(C), DOJ
2:10 PM – 2:25 PM	Break	
2:25 PM – 3:35 PM	Group Activity	(b) (6) OPM Shannon Dahn, FDIC
3:35 AM – 3:50 PM	Break	
3:50 PM – 5:00 PM	Privacy at Government Agencies	Maya Bernstein, HHS

Required Reading

- HEW Report – Summary and Recommendations through page 47:
<https://www.justice.gov/opcl/docs/rec-com-rights.pdf>
- The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection, J. Howard Beales:
<http://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection>
- A-130 Appendix II page 67, Fair Information Practice Principles:
https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf

Suggested Reading

- Overview of Sectoral Approach: <https://www.cdt.org/issue/baseline-privacy-legislation>
- Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," 4 Harv. L. Rev. 193 (1890):
http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html
- OECD Privacy Guidelines: <http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>

Federal Privacy Boot Camp

Week 1



Federal Privacy Council

Introduction to Privacy

- State of Nature: Privacy Self-Governance
- Historical recognition of rights to privacy—Role of individual property rights
- Transition from paper based to electronic information systems – rejection of property.
- Fair Information Practice Principles (FIPPs) and the Privacy Act of 1974.
- Law Enforcement Privacy Principles.
- Information Governance, Social Capital and Trust



Value of Privacy

- Privacy/property rights limit access to persons and their possessions.
- Closely related to human autonomy.
- Confidentiality allows persons to create and maintain social relationships of trust.
- Creation of trust facilitates truthful disclosure.
- Which in turn allows freedom of association and open exchange of ideas.
- Necessary characteristic of civic democracy.

Negative Aspects of Privacy

- Allows people to conceal derogatory information about themselves.
- Allows people to engage in socially disapproved behavior with impunity.
- Impedes truth-finding activity by authorities.
- Taken to extremes, privacy results in Hobbesian states of nature.

Hobbes v. Locke

- For Hobbes, people are not by nature social animals, and society could not exist except by the power of the state. The state of nature is one “of continual fear, and danger of violent death, and life is solitary, poor, nasty, brutish and short.” There is no limit on the power of the state to control individuals.
- For Locke, humans are by nature social animals, know what is right and wrong, and are capable of knowing what is lawful and unlawful well enough to resolve conflicts. As such, there are fundamental limits on the power that a state to control individuals, particularly their consciences, their property, and other fundamental liberties.

Governance of Privacy

- Constitutional Protections
- Statutory Protections
- Regulations
- Voluntary Consensus Industry Standards/Agency Practices and Procedures
- Self-Governance

Information Self-Governance

- During recess, Annie tells her “friend” Sally that she thinks Timmy is cute—that she has a crush on him.
- Sally yells out to all the kids, “Annie loves Timmy, Annie loves Timmy.”
- Annie is mortified, Timmy is embarrassed, Sally gets attention.
- Why doesn’t the teacher intervene?



Self-governing privacy system

- Sally is stigmatized
- Graduated system of sanctions
 - Warning
 - Shunned
 - Self-Help
- Sometimes over punished, sometimes under punished.
- But kids own the system—will not work if Teacher intervenes.
- Result is that kids internalize value of trust.



Principles of Information Governance

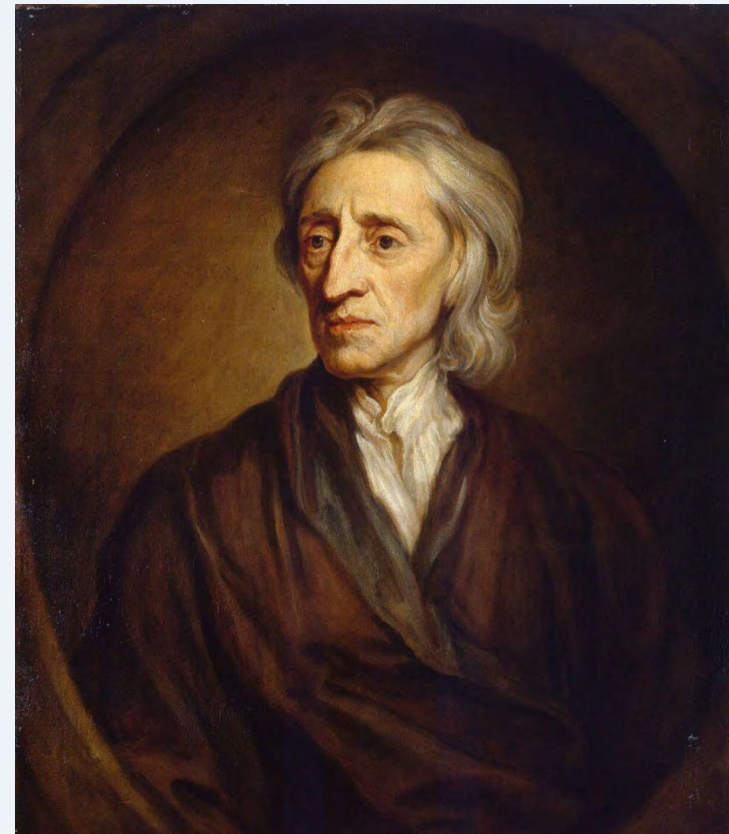
- Information Privacy not about property, it is about people.
- Information Privacy risk is just what people care about.
- Depending on the context, people care about different things.
- What does a system to govern personal information look like?

Historically property rights protected privacy

John Locke (1632 – 1704)

Every man has a property in his own person. This
nobody has a right to, but himself.

- John Locke



Fifth Amendment (1791)

No person . . . shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law.

Fourth Amendment (1791)

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Privacy Protected by Property Rights in Paper

- Mere Evidence Rule
 - Fifth Amendment prevents government from taking property without due process (a trial on the merits).
 - Fourth Amendment applies to contraband or fruits and instrumentalities of crime. Warrant needed to protect against trespass lawsuit by property owner. Exclusionary rule equitable remedy to prevent government from benefiting from violation of property right.
 - Absolute right -- no balancing of risk.
- Privacy is the right of the individual right to control paper-based information, when individual has ownership interest in the paper.
 - Cf. “persons, papers and effects” in Fourth Amendment).

New Information Technology: Telegraph, Telephone

- Invention of the telephone (1876), allowed for near instantaneous communication of electronic information over vast distances.
- Information now in the wires, owned by the communications company, not the sender.
- Property rights ceased to protect individual privacy in electronic information.

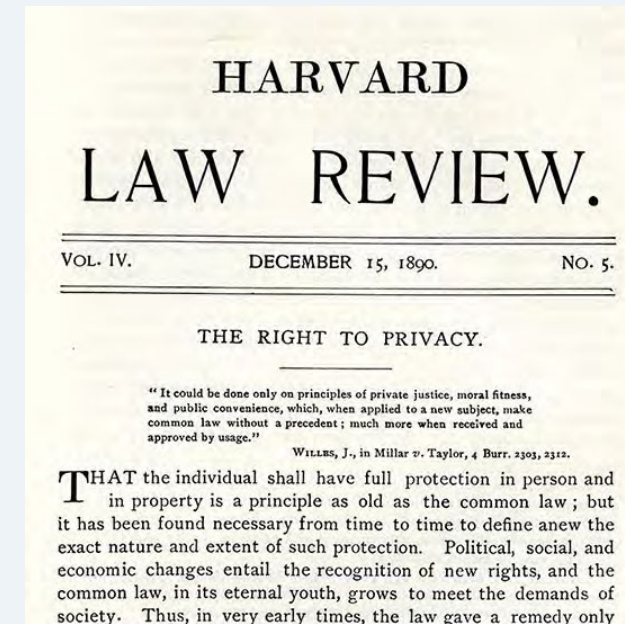


Paper v. Electronic Information

- Paper based information — control over paper gives one control over the information— individual in control of the paper – individual is in control of the information—consent is the framework of governance.
- Information in electronic form, connected to other information, and constantly moving in a system, no longer is within the control of a single individual.

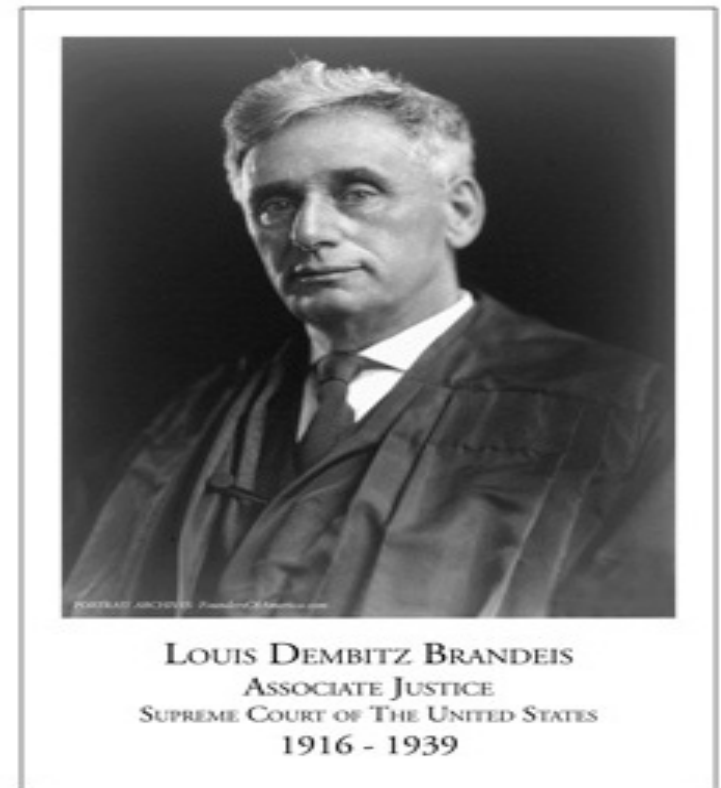
Warren & Brandeis (1890)

- Charles Warren and Louis Brandeis in 1890, Proposed right to privacy not based on real or personal property-modelled on intellectual property right.
- Never adopted as a general common law right—but limited adoption in specific areas of tort law.



Constitutional Right of Privacy?

- Olmstead v. United States (1927), majority refused to suppress evidence obtained through wiretapping finding no trespass/violation of property right
- Brandeis dissented, advocating constitutional acceptance of an individual right of privacy for phone calls on analogy of a letter.
- Brandeis lost because on his view courts could never authorize warrants for search of electronic evidence—implications of the mere evidence rule in Boyd.



Subjective v. Objective

- Property Law – Subjective control over use of a resource – including right to exclude others from access to the resource or transfer one's interest in the resource to others—touchstone is consent.
- Tort Law – Objective duty of care with respect to the handling of a resource – no liability if the duty of care is not breached—touchstone is duty of reasonable care.

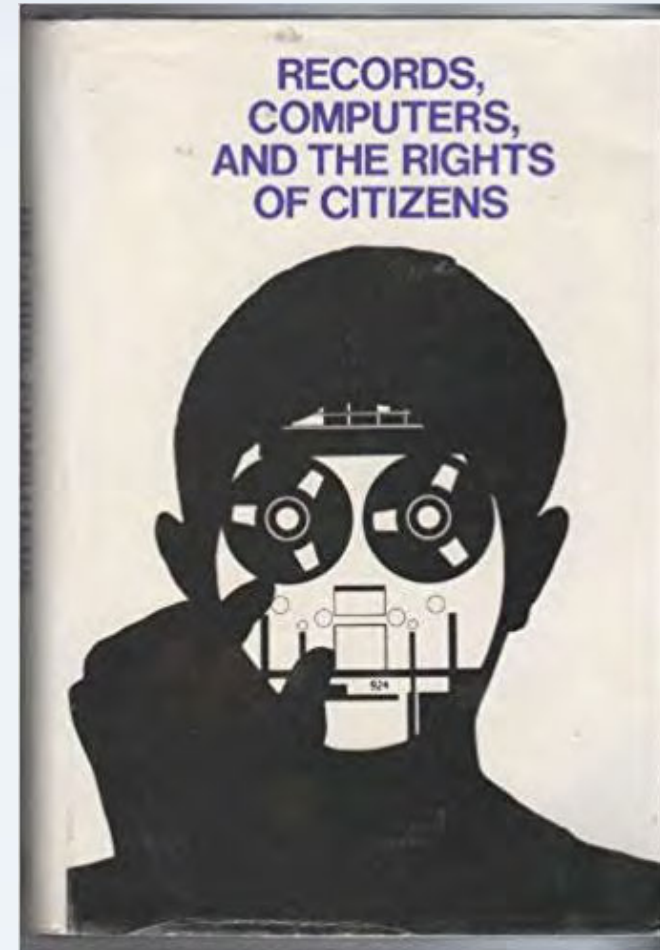
Transformation of the Fourth Amendment

- Warden v. Hayden (1967) – Rejects Mere Evidence Rule.
- Katz v. United States (1967)
Reasonable Expectation of Privacy Test replaces Property Test.
- Determined by what society determined to be reasonable—not individual control.
- Katz rejected Brandeis' attempt to structure privacy on an individual entitlement or property model.



Fair Information Practice Principles (1973)

- Notice
- Primary Use – No Secondary Use without consent
- Access
- Amendment
- Security
- Enforcement



Common Misunderstanding of Fair Information Practice Principles

1 legal concept to rule them all

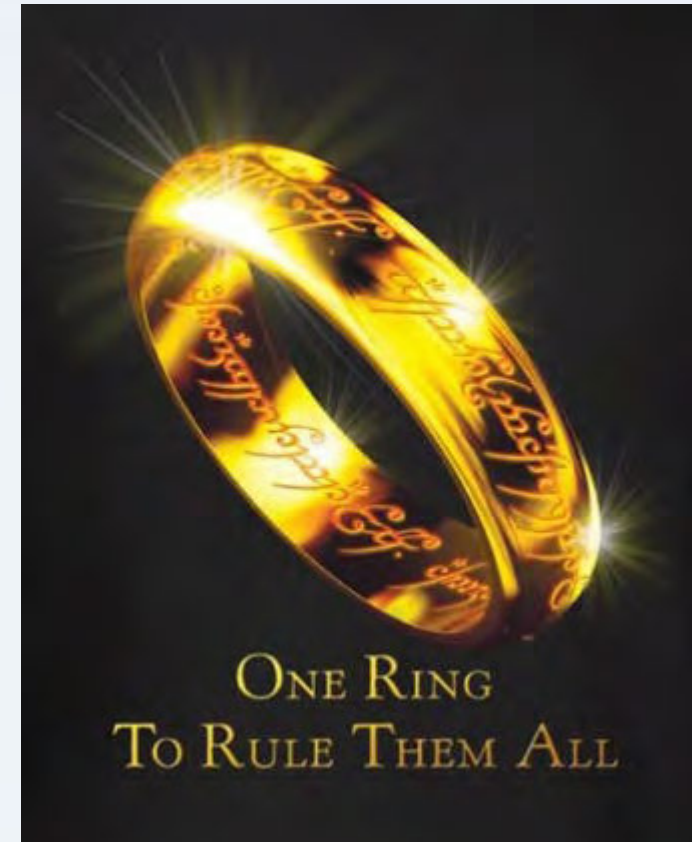
FIPPs: Fair information Practice Principles



@aureliepols

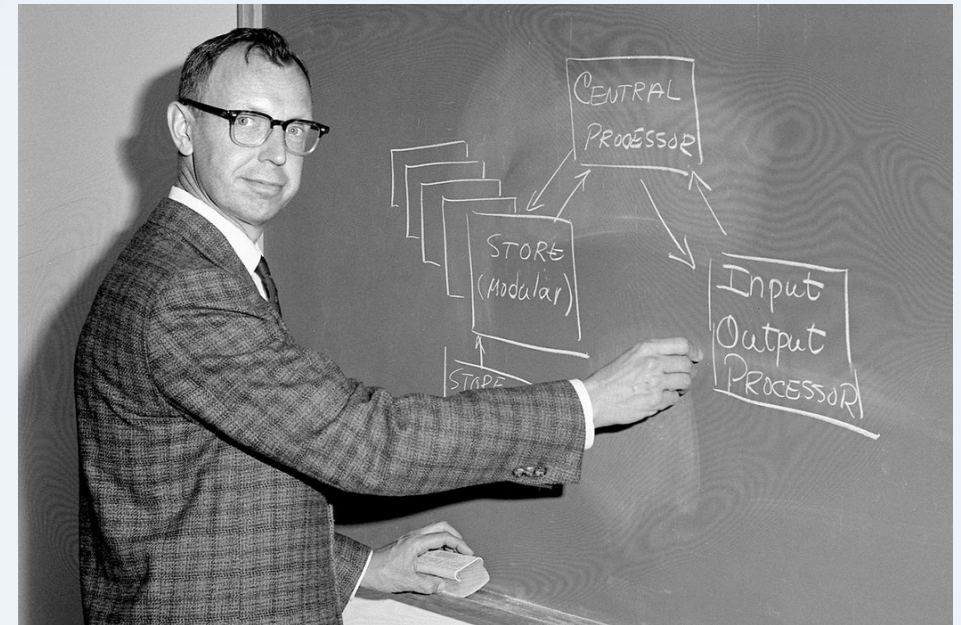
#outfox2015

Stockholm – March 2015



1973 HEW REPORT: COMPUTERS AND THE RIGHTS OF CITIZENS

- Chairman Willis Ware (1920-2013)
Early developer of what became the Internet
- Focus on government benefit programs – Medicare/Medicaid
- Rejects definition of privacy as individual control.
- Privacy redefined as mutuality or trust – protecting shared interests of all stakeholders
- Excluded law enforcement and national security



Historical events

- **Watergate Break In** -- a break-in at the Democratic National Committee (DNC) headquarters
- **COINTELPRO** – surveilling, infiltrating, discrediting, and disrupting American political organizations.
- **IRS Audits:** Thousands of Nixon's political enemies targeted by IRS
 - Second article of impeachment

Privacy Act of 1974

- Based on 1973 HEW Fair Information Practice Principles
- Legislative History makes clear that FIPPs Protect Democracy.
 - Notice
 - Access
 - Amendment
 - Data Security
 - Redress
- Exemptions for Law Enforcement and National Security
 - Confidentiality still required
 - First Amendment Limits
 - Routine uses make consent exception, not the rule.

FIPPs v. Law Enforcement

HEW FIPPs

- Notice – No Secret Systems
- Limits on secondary use
- Access by Data Subject
- Amendment by Data Subject
- Relationship of Trust with Individual

Law Enforcement

- No Notice – Secret Investigations
- Secondary use Encouraged
- No Access by Data Subject
- No Amendment by Data Subject
- Adversarial Relationship with Individual

HEW FIPPs v. Law Enforcement

HEW FIPPs

- Notice
- Limits on secondary use
- Access
- Amendment
- Relationship of Trust with Individual

Law Enforcement Principles

- Constitutional/Statutory Controls:
 - Judicial Authorization for Warrants
 - Public Trials – Transparency
 - Right of Access to exculpatory/impeachment evidence after charges filed.
 - Due Process after charges filed
 - Juries to determine guilt

ATTORNEY GENERAL ELLIOT RICHARDSON

- Secretary of HEW (1971-1973)
Responsible for Fair Information Practice Principles
- Brought HEW Privacy Team to DOJ to Develop Fair Information Practices for Law Enforcement
- Disbanded after Saturday Night Massacre (October, 20, 1973).



Attorney General Guidelines

Attorney General Edward Levi

- First developed for domestic national security investigations, later expanded to all FBI activities, and then applied to intelligence agencies under Sec. 2.3 of Executive Order 12333.
- Response to COINTELPRO Scandal.
- Higher evidentiary thresholds required as investigatory activities became more intrusive.
- Investigations into political activities not permitted without specific and articulable facts suggesting criminal conduct.
- Continuous evidentiary feedback loop to improve guidelines and training.



Statistical Process Controls

Edwards Deming

- During WWII Edwards Demming worked for the War Department to implement modern statistical process controls and industrial standards to achieve legendary reliability of U.S. war equipment.
- Edward Levi was Assistant AG in charge of DOJ's War Division in 1943—when he was trained on standards and statistical process controls—later applied them to the FBI.



Challenge of Information Governance Today

- Personally Identifiable Information – Information that identifies someone, says something about someone, or would if combined with other information.
- Artificial Intelligence and Machine Learning.
- Hayek: Use of Knowledge in Society—Theoretical v. Practical Knowledge.
- How do we govern this common pool resource?

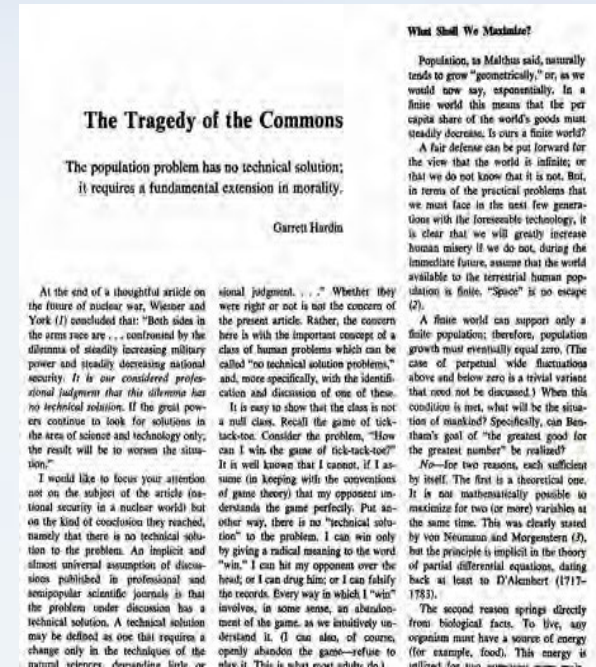
Tragedy of the Commons

Term coined in 1968 Article in Science by Garrett Hardin – Economist – based on an 1833 article by William Forster Lloyd.

Hardin argued unregulated common pool resources (e.g., any common pool resource) will be overused and degenerated to the point that they are no longer sustainable.

Although Hardin's argument was a priori—never subjected to any empirical tests—conventional wisdom in government reduced all questions of governance of common pool resources to a binary choice:

1. Assign property rights to individuals, or
2. Establish administrative “command and control” systems.



Elinor Ostrom

- Empirically tested Hardin's "tragedy of the commons" narrative.
- Established that humans could govern common pool resources without property rights or command and control systems.
- Humans were not trapped and helpless amid diminishing supplies--they could design their own governance systems which were more efficient than "command and control" systems.



“A resource arrangement that works in practice can work in theory.”

Design Principles

- Clearly defined boundaries;
- Context specific/sectoral application of rules;
- Stakeholder participation in design of rules;
- Effective monitoring;
- Graduated sanctions;
- Conflict resolution procedure is accessible and inexpensive;
- Self-governance system recognized by higher-level authorities; and
- In the case of larger common-pool resources, organization in the form of multiple layers of nested enterprises, with small local CPRs at the base level.



Epilogue

Order of the Sacred Treasure, Second Class

- After the war, Detroit rejected Demings' methods – so Deming went to Japan.
- In 1960, Emperor Hirohito awarded Deming the equivalent of a knighthood. The citation on the medal recognizes Deming's contributions to Japan's industrial rebirth and its worldwide success.



PRIVACY 101:

Privacy at a Federal Agency

(b) (7)(C) *Senior Advisor, Privacy Policy*

Department of Homeland Security

September 10, 2021

AGENDA: Privacy at Federal Agencies

- Global Privacy Frameworks
- Federal Privacy Framework:
 - Agency use of PII is governed by:
 - The FIPPs and
 - Privacy law and policy
- Federal Privacy Leadership:
 - OMB
 - Federal Privacy Council
 - Role of the SAOP
 - Privacy stewardship



WHY PRIVACY?



Privacy Stewardship

Effective privacy stewardship includes:

1. **Policy** - Create rules from requirements & principles
2. **Compliance** - Integrate rules into operations using the FIPPs
3. **Oversight** - Verify performance & recommendations
4. **Advocacy** - Teach & share lessons learned
5. **Disclosure/Transparency** - Show results to maintain community trust and support



Global Privacy Frameworks

- Comprehensive Model:
European Union
- Sectoral Model:
United States



The FIPPs in Many Forms

FIPPs-based frameworks have been widely adopted:

- EU Privacy Directive-GDPR
- OECD Privacy Principles
- APEC Privacy Framework
- Canadian PIPEDA
- U.S. Privacy Act
- Other U.S. and State Privacy Laws

More FIPPs



What is PII?

PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

PII can include:

- Your name
- Personal characteristics
- Biometrics
- A unique set of numbers or characters assigned to a specific individual
- Descriptions of event(s) or points in time
- Descriptions of location(s) or place(s)



The Privacy Act of 1974

Purpose is to:

- Balance the government's need to maintain information about individuals with an individuals' right to be protected from unwarranted invasions of their privacy.
- Restrict disclosure of personally identifiable records maintained by the agencies.
- Grant individuals an increased right of access and a right of amendment of records.
- Establish a "code of fair information practices" that regulates the collection, maintenance, use and disclosure of personally identifiable records.
- Grant individuals private rights of action for agency violations of the Act.

E-Government Act of 2002

Purpose is to:

- Ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic government.
- Emphasize the importance of the "development of a comprehensive framework to protect the government's information, operations, and assets."
- Require agencies to conduct Privacy Impact Assessments before developing or procuring new IT that collects, maintains, or disseminations personal information.
- Require privacy policies about information collections.

Legal vs. Policy Distinctions

- Privacy Act:
 - Do I have the LEGAL authority to collect this information
 - Do I have the LEGAL authority to share or disclose information under the SORN?
- E-Gov Act/Agency Privacy Policy:
 - Is it sound policy for the Agency *to collect* this information?
 - Have we appropriately safeguarded it?
 - Have we provided NOTICE beyond what is legally required?



Oversight & Advocacy

Internal oversight:

- Privacy Compliance Reviews
- Federal Advisory Committees (FACA)

External oversight:

- Civil Society
- Inspector General
- GAO
- Congress
- Privacy and Civil Liberties Oversight Board (PCLOB)

The Role of OMB

- The Privacy Act authorized OMB to provide guidance on the Privacy Act, as well as overall leadership and coordination of federal information resources management within the Executive Branch based on recently revised OMB Circular A-130.
- Circular A-130 gathers in one resource a wide range of policy updates for federal agencies regarding cybersecurity, information governance, privacy, records management, open data, and acquisitions. It also establishes general policy for IT planning and budgeting through governance, acquisition, and management of federal information, personnel, equipment, funds, IT resources, and supporting infrastructure and services.

Other OMB Guidance

- OMB Circulars A-130, A-108
- OMB Memoranda (*e.g.*, OMB M-17-12)
- FISMA guidance and annual FISMA reporting metrics

Federal Privacy Council

- Established through Executive Order 13719 to be the principal interagency forum to improve the privacy practices of U.S. Federal Government agencies.
- Works to strengthen protections of people's personal information and privacy rights across the Federal Government.
- Helps U.S. Federal Government agencies to better coordinate and collaborate, educate the federal workforce, and exchange best practices.
- Builds on existing interagency efforts to safeguard PII, and protect the privacy interests of individuals in the information created, collected, used, processed, stored, maintained, disseminated, disclosed, and disposed of by the Federal Government.

Senior Agency Officials for Privacy (SAOP)

OMB issued guidance on the role and designation of SAOPs:

- Requires the head of each agency to assess the management, structure, and operation of the agency's privacy program, and designate or re-designate an official to serve as the SAOP;
- Makes clear that privacy and security are separate disciplines and that the SAOP must serve in a central leadership position and have the necessary authority and expertise to lead the agency's privacy program and carry out all privacy-related functions; and
- Requires the SAOP to take a central role at the agency in policy development and evaluation, privacy compliance, and privacy risk management.

Privacy Stewardship

Effective privacy stewardship includes:

1. **Policy** - Create rules from requirements & principles
2. **Compliance** - Integrate rules into operations using the FIPPs
3. **Oversight** - Verify performance & recommendations
4. **Advocacy** - Teach & share lessons learned
5. **Disclosure/Transparency** - Show results to maintain community trust and support





Federal **P**rivacy **C**ouncil

Federal Privacy Boot Camp

Spring 2022 Agenda Session 2: Privacy Act of 1974

Title Session 2: Privacy Act of 1974

Date March 25, 2022 (Friday)

Location Virtual

Time 1:00 PM - 5:00 PM

Time	Topic	Presenter(s)
1:00 PM – 2:15 PM	Privacy Act	Kirsten Moncada, OMB (b) (6) DoD
2:15 PM – 2:30 PM	Break	
2:30 PM – 3:45 PM	Cont'd	
3:45 AM – 4:00 PM	Break	
4:00 PM – 5:00 PM	Cont'd	

Suggested Reading

- Privacy Act: <https://www.justice.gov/opcl/file/844481/download>

Additional Privacy Act reference materials:

- DOJ Overview of the Privacy Act:
<https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition>
- OMB's Privacy Guidance:
<https://www.whitehouse.gov/omb/information-regulatory-affairs/privacy/>

Attendance and Credit

Boot Camp staff will record attendance via the virtual platform during each session. This record will be used to determine your applicable credits at the conclusion of the training.

- The Federal Privacy Boot Camp qualifies as a training for CLP credit for federal employees. The entire camp is worth 32 credits, 4 per session over 8 sessions.
- If a session ends early, attendees that stay for the full session still earn 4 credits. Those with late arrival or early departure will have credit hours rounded up to the nearest hour.

Should you not be able to attend a session, please give Boot Camp staff advanced notice as soon as possible. If you miss more than two (2) sessions without notice, you will receive a notification that you will be dropped from the Boot Camp if you miss a third.

Session Materials

Weekly emails with slides and materials will be distributed to attendees. Materials will also be posted on the [Privacy Boot Camp MAX page](https://community.max.gov/x/ZwU1S) (<https://community.max.gov/x/ZwU1S>).

Listservs

The Privacy Boot Camp Listserv (privacy-bootcamp@listserv.gsa.gov) has been created to facilitate ongoing discussion during this program. This listserv is not actively moderated and instead will operate as an open forum for discussion. We encourage you to engage with one another through this platform to get to know your privacy peers across Government.

Please email the Privacy Council Inbox (privacy.council@gsa.gov) if you would like to be added as a subscriber to any of the following Privacy Council listservs:

- PRIVACY-COUNCIL: Broadest distribution to the Federal privacy community. Includes a bi-weekly Privacy Post newsletter. General announcements related to the FPC.
- FPC-AIC and AIC-DISCUSSION: List for the Agency Implementation Committee which hosts monthly calls that feature (1) updates from SAOP council meetings, (2) presentations, (3) guided discussions relating to privacy topics, and (4) open Q&A.
- FPC-TI-AI: List for the Artificial Intelligence Working Group within the FPC Technology and Innovation Working Group.
- PRIVACY-JOBS: Subscribers receive and are able to distribute federal privacy job announcements.

Federal Privacy Boot Camp

Session 2



Federal Privacy Council

The Privacy Act of 1974

An Overview

5 U.S.C. §552a



Agenda

1. What is Privacy as it relates to federal government information?

Scope of Privacy Act

Systems of Records



2. How do federal agencies disclose records under the Privacy Act?

Disclosure Prohibition

12 Exceptions to the Rule



3. What are federal agencies required to do?

Requirements, Rights

Exemptions

1. WHAT IS PRIVACY



Historical context



The Watergate Scandal and other allegations of governmental abuse led Congress to pass the Privacy Act of 1974.

What is the purpose of the Privacy Act?



To balance the Government's need to maintain information about individuals with the rights of those individuals to be protected from unwarranted invasions of their privacy

Basic Policy Objectives of the Privacy Act

1. Restrict disclosure of personally identifiable records maintained by agencies
2. Grant individuals an increased right of access and a right of amendment
3. Establish a “code of fair information practices” that regulates collection, maintenance, use, and disclosure
4. Grant individuals private rights of action for agency violations of the Act

Key Definitions



- The Privacy Act is a technical statute
- Definitions dictate whether the statute applies

For Example

- Who is required to comply with the Privacy Act?
- Who can utilize the Privacy Act?
- What does the Privacy Act pertain to?



Who Must Comply? Federal Agencies

Also ➡ Subsection (m) government contractors

- PA requirements apply if contract is for operation of a system of records to accomplish an agency function
- For purposes of criminal penalties, subsection (m) contractors are considered to be agency employees
- Federal Acquisition Regulation sets forth language that must be inserted in solicitations and contracts for design, development, or operation of a system of records (48 C.F.R. § 24.104)



Section 7 applies to State and local agencies - SSNs

- Unlawful for any Federal, State, or local agency to deny a right, benefit, or privilege provided by law because of an individual's refusal to provide his/her SSN.
 - *EXCEPT* where disclosure is required by Federal statute, or
 - agency system operated before 1975 to verify identity per statute or regulation.
- Any Federal, State, or local agency requesting SSN is required to inform
 - whether disclosure is mandatory or voluntary,
 - under what statutory or other authority SSN is solicited
 - what uses will be made of the SSN



Who can use the Privacy Act?

Under the Privacy Act's Definition

Individual = U.S. Citizen or Lawful Permanent Resident

NOT covered by the Privacy Act?

- Deceased persons
- Corporations and organizations
- Non-citizens or non-lawful permanent residents

What does the Privacy Act pertain to?

***Records
in a
System of Records***

Privacy Act Records

Personnel Record

PERSONNEL RECORD

Name: _____ W. I. _____
Address: _____
City and State: _____ Phone No. _____ Date of Birth: _____ Sex: _____
Marital Status: _____ Date of Birth: _____ Date of Dependency: _____
Date Employed: _____ Department: _____ Starting Rate: _____
Occupational Classification: _____
Education and Previous Working Experience: _____

No.	Date of Birth	Reason for Change	Authorized By

State Job Order: _____ Reason for Issuing: _____

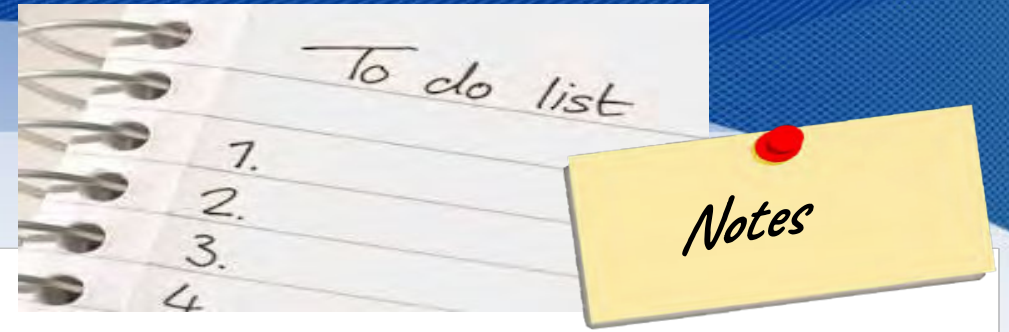


Any item, collection, or grouping of information about an individual that is maintained by an agency and that contains his/her name or an identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint, voiceprint, or photograph

KEY POINTS

- Must be about the individual
- Must identify the individual
- Must be maintained by an agency

Personal Notes



Purely personal notes – generally, NOT considered to be covered by the Privacy Act

Supervisor's personal notes – memory refreshers

- To remain personal:
 - Must be kept and maintained only for personal use of the supervisor
 - Must NOT be circulated to anyone
 - Must NOT be under the control of the agency or required by the agency to be maintained
- Duty to incorporate personal notes if used in an adverse determination about an individual

Privacy Act Records in a **SYSTEM OF RECORDS**



*SYSTEM OF RECORDS – A group of any records under the control of any agency from which information **is retrieved by** the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.*

Coverage under the Privacy Act depends on the method of retrieval, rather than solely the content of the record.

Standard: Actual Retrieval



OMB Guidelines

A system of records exists if:

- 1) there is an indexing or retrieval capability using identifying particulars built into the system
and
- 2) the agency does, in fact, retrieve records about individuals by reference to some personal identifier

System of Records – Why is this definition so important?

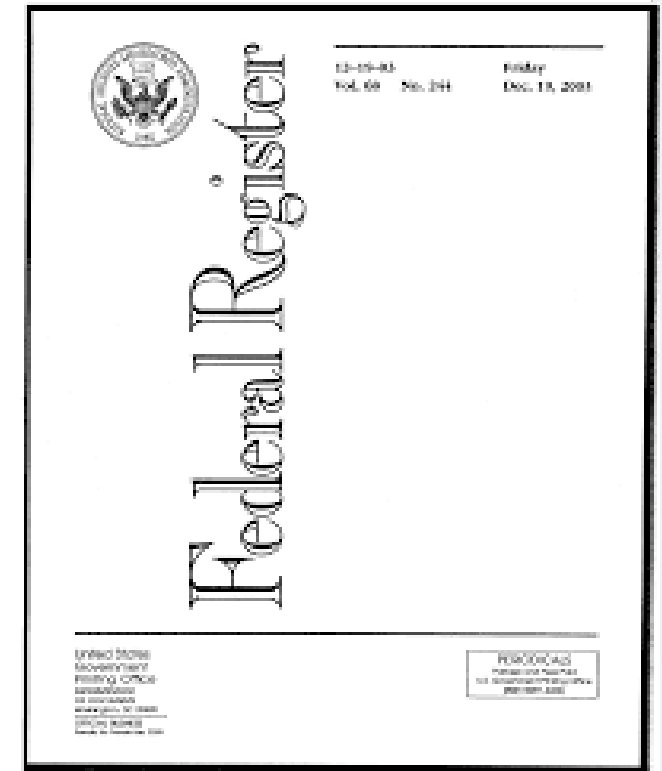
- Most of the rights and requirements of the Privacy Act depend on whether this definition is met
 - *For ex., wrongful disclosure suits, access and amendment rights*
- *Notice Requirements*
 - Must publish a system of records notice in the Federal Register (5 U.S.C. § 552a(e)(4))
 - OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act



FEDERAL REGISTER
The Daily Journal of the United States Government

System of Records Notice (SORN)

- ❖ System name and number
- ❖ Security classification
- ❖ System location
- ❖ System manager(s)
- ❖ Authority for maintenance
- ❖ Purpose
- ❖ Categories of individuals
- ❖ Categories of records
- ❖ Record source categories



SORNs (continued)

- ❖ Routine uses, including categories of users and purposes of uses
- ❖ Policies and practices for storage
- ❖ Policies and practices for retrieval
- ❖ Policies and practices for retention and disposal
- ❖ Administrative, technical, and physical safeguards
- ❖ Record access procedures
- ❖ Contesting record procedures
- ❖ Notification procedures
- ❖ Exemptions
- ❖ History



2. DISCLOSURE OF RECORDS

Rule: No Disclosure without Consent



“No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.” 5 U.S.C. § 552a(b)

12 Exceptions to the Rule

- 1. Intra-agency disclosures: “Need to know”**
- 2. Required by the FOIA**
 - FOIA request in hand
 - No discretionary disclosures
- 3. Routine Use**
 - Published in agency SORN
 - Disclosure compatible with purpose for collection
- 4. Bureau of the Census**
- 5. For statistical research or reporting**
- 6. NARA**

12 Exceptions to the Rule (cont'd)

7. **Written request** by the head of a **government agency** or instrumentality within/under the control of the **US** for an authorized civil or criminal **law enforcement** activity
8. **Compelling circumstances** affecting the **health or safety** of an individual (notice required)
9. **Congress**
10. **Comptroller General/GAO**
11. **Court Order**
12. **Debt Collection Act**

Accounting of Certain Disclosures

Each agency shall:

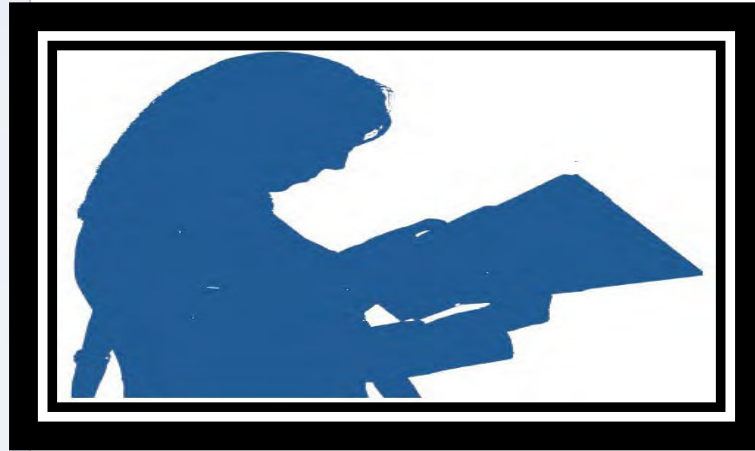
Maintain an accounting of disclosures from a system of records except for disclosures made:

- Under (b)(1) – need to know within the agency
- Under (b)(2) – FOIA

Make the accounting available to the record subject, except for disclosures under (b)(7) – law enforcement.

Use accountings to inform any person or agency to which a record has been disclosed about any correction to the record or notation of dispute.

Access to Records



- Privacy Act provides the record subject with an **independent right of access** to records in a SOR
- Privacy Act access is **independent of, and in addition to,** access rights available under **FOIA**

The Freedom of Information Act

A Quick Look

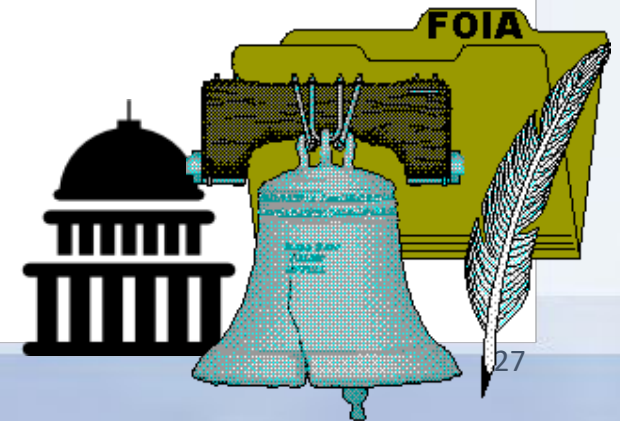
5 U.S.C. §552



The Freedom of Information Act (FOIA)

5 U.S.C. § 552

- Gives any person the right to request Federal agency records. It also requires Federal agencies to affirmatively make certain types of information available to the public.
- *Who?* – Anyone can make a FOIA request (individuals, corporations, organizations)
- *What?* – Any agency records may be requested (paper documents, emails, audio and video recordings, and other electronic records)
- *Why?* – The basic purpose of FOIA is to ensure an informed citizenry; hold the governors accountable to the governed.



How does FOIA work?

- Federal agencies are required to make certain records available to the public proactively and in response to FOIA requests.
- Federal agencies are required to disclose information unless it falls under one of the *9 exemptions*, which protect interests such as personal privacy, national security, and law enforcement.
- Agencies may only withhold information under the FOIA if the agency reasonably foresees that disclosure would harm an interest protected by an exemption or where disclosure is prohibited by law.
- Where full disclosure of a requested record is not possible – agencies are to consider partial disclosure and take reasonable steps to segregate and release non-exempt information.

The image shows two pages of a document, likely a CIA memo, with classification markings and redacted content. The top page has a classification marking of 'TOP SECRET' and 'CONFIDENTIAL'. The bottom page has a classification marking of 'CONFIDENTIAL'. The document contains several paragraphs of text, many of which are redacted with black boxes. The text appears to be a report or memo, possibly related to the Vietnam War, as mentioned in the text. The document is dated 'FEBRUARY 1, 1961' and is addressed to 'DIRECTOR, CIA'.

FOIA and Privacy

- 2 exemptions that protect privacy
 - Exemption 6
 - Exemption 7(C)
 - *Both encompass information that is inherently private, as well as the concept of privacy in terms of an individual's control of information concerning him/her.*
- 2 areas of interface with the Privacy Act
 - *1st Party Access situation – independent, additional means of access*
 - *3rd Party Access situation – restricts access*
- Segregation of nonexempt information
 - *De-identification*

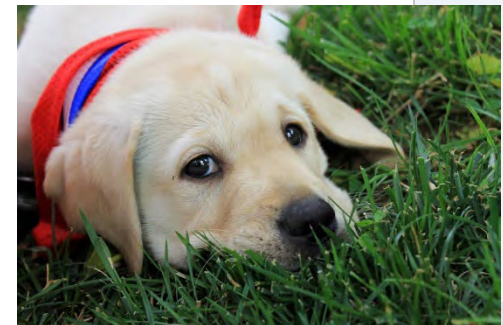


Amendment of Records

- Individuals may request amendment of their records
- Standard = such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual about making a determination about him/her
- Appeal and statement of disagreement
- Notification of subsequent disclosures
- Notification to prior recipients
- Facts versus opinions



- **Knowledge Check:** Your colleague is new to privacy and works in the agency FOIA office. She has a request from an individual for records about the individual that are maintained in the agency's contract files. The agency maintains and retrieves the contract files by contract numbers.
- There is PII in these files, such as names and home addresses, that may reveal information about an individual.
- Your friend asks you whether this should be processed under the FOIA or the Privacy Act. What would you advise? Why?



3. AGENCY REQUIREMENTS



What are agencies required to do under the Privacy Act?

- (e)(1) – Maintain only relevant and necessary information to accomplish a purpose of the agency required by statute or EO
- (e)(2) – Collect information from the record subject when information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs
- (e)(3) – Inform each individual when collecting information of: the authority, the principal purpose(s) for which the information is to be used, routine uses, and effects, if any, of not providing the information

Agency Requirements (cont'd)

- (e)(4) – Publish system notice in the Federal Register
- (e)(5) – Maintain all records which are used in making any determination about an individual with such accuracy, relevance, timeliness, and completeness to assure fairness to the individual
- (e)(6) – Prior to disseminating any record to any person other than an agency, unless required by FOIA, make reasonable efforts to assure records are accurate, complete, timely, and relevant for agency purposes

- **Knowledge Check:** Human Resources staff generate an extract of personnel data from an HR system listing those with upcoming within-grade-increases and career-ladder promotions for all organizations within a component. The purpose is to have supervisors review and verify the information is correct before those actions occur.
- The PII data fields extracted onto a spreadsheet are Employee Name, Date of Birth, and Social Security Number. (The spreadsheet also contains the required WGI/CLP data supervisors must verify.)
- Before it is sent to supervisors to your agency components, you are asked to review the spreadsheet for privacy concerns. **I know you spot some potential record disclosure issues, but what record keeping issues do you spot based on what you just learned?**

WARNING:
TOO MUCH
INFORMATION CAN HARM

Agency Requirements (cont'd)

- (e)(7) – Maintain no record describing how an individual expresses 1st Amendment rights unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity
- (e)(8) – Make reasonable efforts to serve notice when any record is made available to any person under compulsory legal process when such process becomes a matter of public record

Agency Requirements (cont'd)

- (e)(9) – Establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and provide instruction for each such person regarding the rules, the Privacy Act's requirements, and the penalties for noncompliance
- (e)(10) – Establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained

Agency Requirements (cont'd)

- (e)(11) – At least 30 days prior, publish in the Federal Register notice of any new use or intended use of the information, and provide an opportunity for interested persons to submit comments
- (e)(12) – At least 30 days prior to establishing or revising a computer matching program with a non-Federal agency, publish notice of such establishment or revision in the Federal Register

Computer Matching

- Privacy Act sections (a)(8)-13, (e)(12), (o), (p), (q), (r), and (u).
- What is a “matching program”?
- *Federal Register* notice
- Matching agreements
- Due process
- Data Integrity Boards



10 Exemptions: Limitations of Rights

(d)(5) – exemption from **access only** of information compiled in reasonable anticipation of a civil action or proceeding

- Similar in some respects to attorney work product privilege
- Not limited to information compiled for judicial proceedings, but also covers administrative hearings

10 Exemptions (cont'd)

Subsection (j) – regulation required

(j)(1) – information maintained by the CIA

(j)(2) – information maintained by a principal function criminal law enforcement agency and compiled for criminal law enforcement purposes

- Is the agency a criminal law enforcement agency?
- If so, was the information compiled for criminal law enforcement purposes?

10 Exemptions (cont'd)

Subsection (k) – regulation required

(k)(1) – classified information

(k)(2) – investigatory material compiled for law enforcement purposes, other than material within scope of (j)(2)

2 elements

- Is the material investigatory material not covered by (j)(2), for example, civil or regulatory enforcement
- Was an individual denied a right, privilege, or benefit as a result of the maintenance of the records?

If so, then the exemption only protects information that would reveal a source provided an express promise of confidentiality.

10 Exemptions (cont'd)

(k)(3) – maintained in connection with providing protective services to the President or other individuals

(k)(4) – required by statute to be maintained and used solely as statistical records

(k)(5) – information that reveals a source provided an express promise of confidentiality in the context of background investigatory material to determine eligibility for Federal employment, military service, Federal contracts, or access to classified information

(k)(6) – testing material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness or the testing process

(k)(7) – information that reveals a source provided an express promise of confidentiality in the context of evaluation material used to determine potential for promotion in the armed services

- **Knowledge Check:** You have just drafted a new system of records notice for a department-wide system that covers records that are compiled for an all agency new insider threat program. Some of the information will be compiled for a law enforcement purpose.
- What are some considerations you need to think of for drafting the exemption regulation?

Civil Remedies



1. Amendment lawsuits
2. Access lawsuits
3. Accuracy lawsuits for damages
4. Other damages lawsuits
 - wrongful disclosure, wrongful maintenance, or any other violation of the Privacy Act that results in an adverse effect on an individual

Criminal Penalties



Misdemeanor and fine up to \$5000:

- Any officer or employee who knowingly and willfully disclosures individually identifiable information to any person not entitled to receive it
- Any officer or employee who willfully maintains a SOR without meeting the notice requirement
- Any person who knowingly and willfully requests or obtains a record concerning an individual under false pretenses

Privacy Act Resources

- ✓ Agency SAOPs, CPOs, Privacy Act Officers
- ✓ OMB privacy guidance and reference materials, including its Privacy Act Implementation Guidelines, available at:
https://www.whitehouse.gov/omb/privacy_general
- ✓ DOJ/Office of Privacy and Civil Liberties, “Overview of the Privacy Act of 1974,” available at: www.justice.gov/opcl
- ✓ Federal Privacy Council



Federal Privacy Council

Federal Privacy Boot Camp

Spring 2022 Agenda Session 3: PIAs, FIPPs & Reporting

Title Session 2: Privacy Assessments, Implementing the FIPPs, and Reporting

Date April 1, 2022 (Friday)

Location Virtual

Time 1:00 PM - 5:00 PM

Time	Topic	Presenter(s)
1:00 PM – 2:15 PM	Privacy Impact Assessments (PIAs)	Kellie Cosgrove Riley, OPM (b) (7)(C) NSA
2:15 PM – 2:30 PM	Break	
2:30 PM – 3:45 PM	Fair Information Practice Principles (FIPPs)	
3:45 AM – 4:00 PM	Break	
4:00 PM – 5:00 PM	Cont'd	

Required Reading

- E-Government Act and Relevant OMB Guidance:
<https://www.justice.gov/opcl/e-government-act-2002>
- NIST 800-53 Appendix J, Starting at Page 437:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>
- Data Mining Law, 803 and 804 of IRPTA:
<http://dpcl.d.defense.gov/Portals/49/Documents/Civil/Sec803.pdf>

Attendance and Credit

Boot Camp staff will record attendance via the virtual platform during each session. This record will be used to determine your applicable credits at the conclusion of the training.

- The Federal Privacy Boot Camp qualifies as a training for CLP credit for federal employees. The entire camp is worth 32 credits, 4 per session over 8 sessions.
- If a session ends early, attendees that stay for the full session still earn 4 credits. Those with late arrival or early departure will have credit hours rounded up to the nearest hour.

Should you not be able to attend a session, please give Boot Camp staff advanced notice as soon as possible. If you miss more than two (2) sessions without notice, you will receive a notification that you will be dropped from the Boot Camp if you miss a third.

Session Materials

Weekly emails with slides and materials will be distributed to attendees. Materials will also be posted on the [Privacy Boot Camp MAX page](https://community.max.gov/x/ZwU1S) (<https://community.max.gov/x/ZwU1S>).

Listservs

The Privacy Boot Camp Listserv (privacy-bootcamp@listserv.gsa.gov) has been created to facilitate ongoing discussion during this program. This listserv is not actively moderated and instead will operate as an open forum for discussion. We encourage you to engage with one another through this platform to get to know your privacy peers across Government.

Please email the Privacy Council Inbox (privacy.council@gsa.gov) if you would like to be added as a subscriber to any of the following Privacy Council listservs:

- PRIVACY-COUNCIL: Broadest distribution to the Federal privacy community. Includes a bi-weekly Privacy Post newsletter. General announcements related to the FPC.
- FPC-AIC and AIC-DISCUSSION: List for the Agency Implementation Committee which hosts monthly calls that feature (1) updates from SAOP council meetings, (2) presentations, (3) guided discussions relating to privacy topics, and (4) open Q&A.
- FPC-TI-AI: List for the Artificial Intelligence Working Group within the FPC Technology and Innovation Working Group.
- PRIVACY-JOBS: Subscribers receive and are able to distribute federal privacy job announcements.

Federal Privacy Boot Camp

Session 3



Federal Privacy Council

Agenda

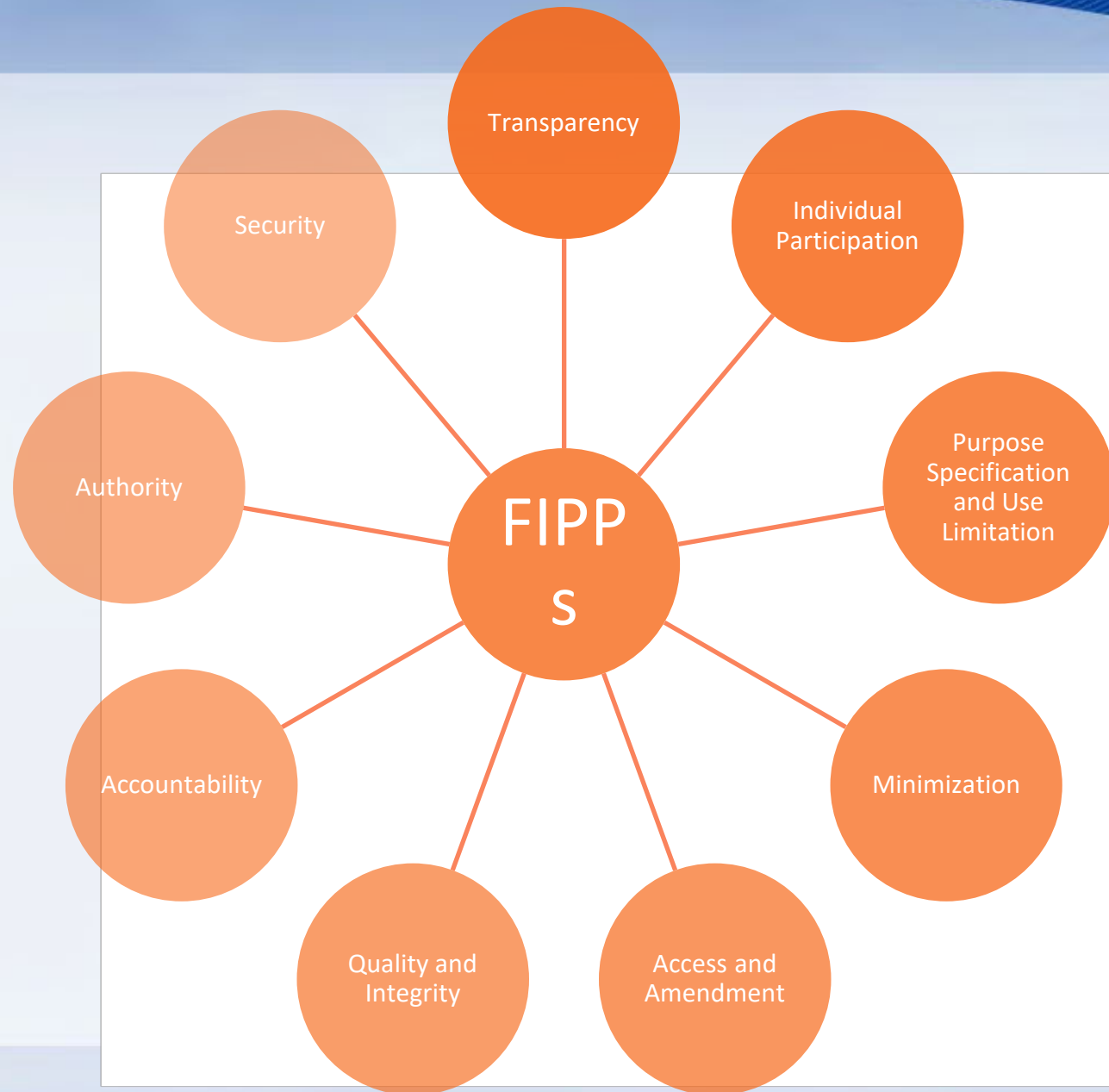
- Introduce the Fair Information Practice Principles
- Understand the Role of Privacy Impact Assessments
- Practice Applying the FIPPs

Fair Information Practice Principles

- Fair information practice principles were first articulated in a comprehensive manner in the United States Department of Health, Education and Welfare's 1973 report entitled *Records, Computers and the Rights of Citizens* (1973), known as the *HEW Report*
 - The *HEW Report* led the passage of the U.S. Privacy Act of 1974
- FIPPs based frameworks adopted worldwide:
 - OECD Privacy Principles
 - APEC Privacy Framework
 - U.S. Privacy Act
 - Canadian PIPEDA

FIPPs Come in Many Forms

- Federal Trade Commission
- Department of Homeland Security
- National Strategy for Trusted Identities in Cyberspace (NSTIC)
- A-130 Appendix II



How do you use the FIPPs

- FIPPs as the foundational principles for privacy policy and implementation
- Provides a consistent approach to analysis of the privacy issues

Authority

- Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have the authority to do so, and should identify this authority in an appropriate notice.
- Federal Government must be given the authority to conduct an activity either through the Constitution or Congress.
 - Statute
 - Regulation
 - Executive Order

Transparency (Notice)

- Agencies should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.
- Examples of transparency:
 - A Privacy Act Statement on a form at time of collection
 - Privacy Impact Assessments published on website
 - Signs that say “this area under Closed Circuit TV”

What is adequate notice?

- A homeowner from Louisiana is filing for housing benefits with Federal Agency. The homeowner is required to enter her PII and property information into an online form on www.federalagency.gov.
 - How can the Agency provide notice to the homeowner about why her information is being collected?
- What if she wants to call the Agency phone helpline instead?

What is adequate notice?

- Agency has cameras filming any travelers that are waiting in line at the airport security checkpoints. Individuals do not fill out a form prior to passing through the checkpoint.
 - On what type of individuals do these cameras capture information?
 - How can an Agency provide notice?
 - Is this notice adequate?

Group Exercises – Applying the FIPPs in Practice

- We will do the first exercise together.
- The second exercise, you will be separated into rooms.
 - You will be given 5 minutes to answer the questions on the next slide.
 - Pick a leader to speak and take notes. Content in breakout rooms will be lost when we return to the main room.
 - When we come back, we will call on two groups to voice their answers.

Group Exercise 1

- Agency A is creating a new program to send people to Mars.
 - They decide to put up materials and ask for anyone interested in the program to subscribe online to get information and updates.
 - Each day they send out updates.
 - They decide to build up interest in the program on social media – creating a Facebook, Instagram, Snapchat, and Twitter accounts.
-
- **Provide two examples of where Agency could find their authority**
 - **Provide three examples of notice/transparency**
 - **What are some pitfalls that you need to watch for?**

Group Exercise 2

- As Agency A moves into the next phase of finding individuals interested in going to Mars, they decide to ask for applicants and ask for more in depth information to identify qualified applicants.
- They decide to create an online application tool, where applicants can see where they are in the process. In order to create the online application tool, Agency A contracts out to Contractor Company B. Agency A decides to do a identify verification process.
- In your small group:
 - **Provide two examples of where Agency could find their authority**
 - **Provide three examples of notice/transparency**
 - **What are some pitfalls that you need to watch for?**

Individual Participation

- Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII. Agencies should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.
- Examples of individual participation:
 - Providing information to request a retirement benefit
 - Applying for a trusted traveler or other credential
 - Being booked by a law enforcement agency
- Privacy Risk is greater whenever information is NOT collected directly from the individual.

Is there adequate individual participation?

- Federal Agency has set up a disaster relief center following a hurricane. Trying to be helpful, a neighbor offers to fill out benefit forms for all of the families on his street since he knows their contact information.
 - Can the Agency accept these forms?
- What about...
 - Disability benefit forms filled out by a guardian/attorney on behalf of the individual?
 - Fingerprints taken for a background investigation?
 - A report filed under the “See Something Say Something” campaign?

Access and Amendment

- Agencies should provide individuals with appropriate access to PII and appropriate opportunity to correct or amend PII.
 - Redress is a critical part of the Privacy Act.
 - Privacy Act grants individuals the right to correct, amend and access records about themselves that the government maintains
 - Privacy Act Request

Is there Access and Amendment?

- A candidate for employment with the federal government is denied a security clearance, and therefore is not granted employment. The candidate files a Privacy Act request to determine what information was gathered about him, and why he failed the background investigation.
 - What records can we provide?
- As it turns out, the candidate's name is John Smith, and his birth date was transcribed when entered into the eQIP process. Mr. Smith files an action to correct and amend his records.

Is there Access and Amendment?

- An individual submits a request for a benefit. The individual inputs the wrong email address.
 - How can we set up a system so that the individual can have direct access?
 - Are there instances where direct access may not be appropriate?

Group Exercise 1

- Agency A is creating a new program to send people to Mars.
- They decide to put up materials and ask for anyone interested in the program to subscribe online to get information and updates.
- Each day they send out updates.
- They decide to build up interest in the program on social media – creating a Facebook, Instagram, Snapchat, and Twitter accounts.
- **Provide two examples of how you could meet the requirement to have individual participation.**
- **Provide an example of how you could provide access and amendment.**

Group Exercise 2

Exercise 2

- As Agency A moves into the next phase of finding individuals interested in going to Mars they decide to ask for applicants and ask for more in depth information to identify qualified applicants.
- They decide to create an online application tool, where applicants can see where they are in the process. IN order to create the online application tool, Agency A contracts out to Contractor Company B. Agency A decides to do a identify verification process.
- In your break out rooms answer the following:
 - **Provide two examples of how you could meet the requirement to have individual participation.**
 - **Provide an example of how you could provide access and amendment.**

Purpose Specification and Use Limitation

- Agencies should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.
- Example:
 - COVID-19 positive testing is used *only* by medical personnel for contact tracing within a federal facility.
 - Benefits enrollment information is *only* used for the benefit for which you applied
 - Disaster relief information is used for disaster relief purposes

Purpose Specification and Use Limitation

A federal agency collects biometric information to support the two factor authentication of a Trusted Traveler Card.

- A State government wants to verify the identity of persons entering its State House and requests access to the federal biometric holdings. Is this permissible?
- Another federal agency wants to vet the identity of volunteers for its own purposes. In what instances, if any, might this be permissible?

Purpose Specification and Use Limitation

- Use of “pattern based analysis” queries on large amounts of existing data.
- Data Mining/Big Data/Machine Learning/Artificial Intelligence – why does it matter?



Minimization

- Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only retain PII for as long as is necessary to accomplish the purpose.
- In application:
 - Minimize use of social security number
 - Programs should collect only the **minimum amount of information necessary to accomplish their mission**
 - Retain information minimum amount of time necessary to accomplish mission

Minimum PII necessary?

- SSN on HR change of address form?
- SSN to sign up to take a class through your online training tool?
- SSN to sign up to take a class outside your agency?
- SSN to book a flight through an airline?

Minimization - Retention

- Agency is performing temperature testing on anyone entering the federal facility.
 - Do you need to collect the temperature at all?
- Contrast this with health information for a clinical study.

Group Exercise 1

- Agency A is creating a new program to send people to Mars.
- They decide to put up materials and ask for anyone interested in the program to subscribe online to get information and updates.
- Each day they send out updates.
- They decide to build up interest in the program on social media – creating a Facebook, Instagram, Snapchat, and Twitter accounts.
- **Provide two examples of how you address data minimization.**

Group Exercise 2

- As Agency A moves into the next phase of finding individuals interested in going to Mars they decide to ask for applicants and ask for more in depth information to identify qualified applicants.
- They decide to create an online application tool, where applicants can see where they are in the process. In order to create the online application tool, Agency A contracts out to Contractor Company B. Agency A decides to do a identify verification process.
- In your group:
 - **Provide two examples for data minimization.**

Quality and Integrity

- Agencies should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.
- Example:
 - Benefits determinations
 - Law enforcement activities
 - Intelligence Community

Quality and Integrity Risks?

- Analyst at Agency 1 reviews information at Agency 2 and manually enters missing information.
 - What are some of the data quality risks with this model?
- Analysts search social media using designated search terms to develop situational awareness reports.
 - What are some of the data quality risks with this model?

Security

- Agencies should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.
- Examples:
 - Technical controls on data
 - Role-based access to data

Accountability

- Agencies should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define the roles and responsibilities with respect to PII for employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.
- Examples:
 - Building in privacy compliance reviews
 - Strong audit capabilities in the data

Security and Accountability Example

- What if an employee is curious about President's travel history?
Can an Agency take steps to safeguard records from unauthorized access?
- Mitigation tools:
 - Employee training about “need to know”
 - Robust audit trails to check who accessed what data and when
 - Alerts to supervisors if sensitive data inappropriately accessed
 - Remedial training for employees

Group Exercise 1

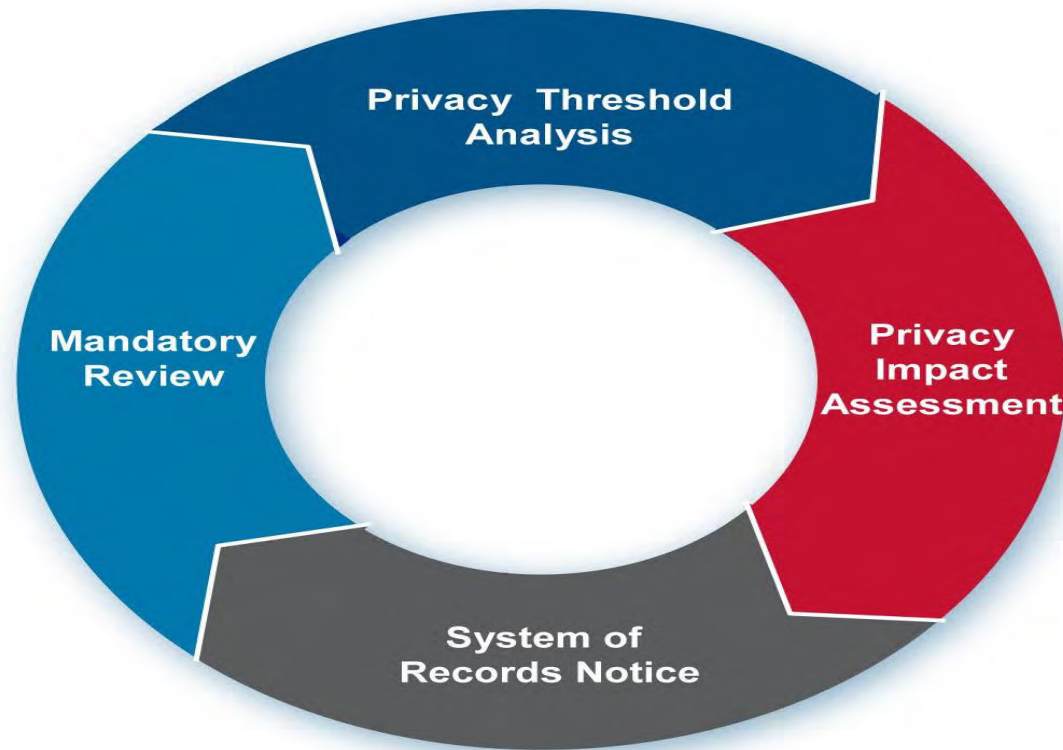
- Agency A is creating a new program to send people to Mars.
- They decide to put up materials and ask for anyone interested in the program to subscribe online to get information and updates.
- Each day they send out updates.
- They decide to build up interest in the program on social media – creating a Facebook, Instagram, Snapchat, and Twitter accounts.
- **Provide one example of a data quality and integrity control.**
- **Provide two examples of accountability controls.**
- **Provide two examples of security controls.**

Group Exercise 2

- As Agency A moves into the next phase of finding individuals interested in going to Mars they decide to ask for applicants and ask for more in depth information to identify qualified applicants.
- They decide to create an online application tool, where applicants can see where they are in the process. In order to create the online application tool, Agency A contracts out to Contractor Company B. Agency A decides to do a identify verification process.
- In your group:
 - **Provide one example of a data quality and integrity control.**
 - **Provide two examples of accountability controls.**
 - **Provide two examples of security controls.**

Privacy Compliance Process

The FIPPs in Action



Privacy Assessments

- **E-Government Act of 2002, Section 208 and OMB M-03-22**
 - Ensures sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic government.
 - Emphasizes the importance of the "development of a comprehensive framework to protect the government's information, operations, and assets."
 - Requires agencies to conduct PIAs.
- **Other Privacy Assessments**
 - Rulemakings
 - National Security Systems
 - Other programmatic privacy assessments

The E-Government Act of 2002

PIA requirements

- Requires agencies to conduct PIAs *before*:
 - Developing or procuring new IT that collects, maintains, or disseminations personal information
 - Any new collections (regardless of IT form):
 - ✓ Collected, maintained or disseminated by IT; or
 - ✓ From 10 or more members of the public (PRA standard)

Compliance Artifacts

Privacy Act of 1974

SORNs

NPRMs

Final Rules

e(3) statements

CMAs

E-Gov Act of 2002

PIA

**Web privacy
policy**

Policy

PTA

Privacy Impact Assessment (PIA)

- PIA is a decision-making tool used to identify and mitigate privacy risks at the beginning of and throughout the development life cycle of a program or system. It helps the public understand what PII is being collecting, why it is being collected, and how it will be used, shared, accessed, secured and stored.
- PIA uses the Fair Information Practice Principles (FIPPs) to assess and mitigate any impact on an individual's privacy. Generally, a PIA is required before a program or system containing PII becomes operational.

There are many reasons for conducting a PIA, which include:

- When developing or procuring any new Department program or system that will handle or collect PII
- For budget submissions to the Office of Management and Budget (OMB) that affect PII
- With pilot tests that affect PII
- When developing program or system revisions that affect PII
- When issuing a new or updated rulemaking that involves the collection, use, and maintenance of PII

Privacy Impact Assessments

- A successful PIA should accomplish two goals:
 - Determine the **risks and effects**; and
 - Evaluate **protections** and alternative processes to **mitigate potential privacy risks**.

Process and Document

- **Iterative process** with program, legal counsel, IT and Privacy Office collaborating
- **Start at the beginning** of a new program and **build in privacy**

Does your agency have a PIA Template?

At a minimum a PIA must have the following – based on OMB 03-22

- what information is to be collected (e.g., nature and source);
- why the information is being collected (e.g., to determine eligibility);
- intended use of the information (e.g., to verify existing data);
- with whom the information will be shared (e.g., another agency for a specified programmatic purpose);
- what opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent;
- how the information will be secured (e.g., administrative and technological controls⁷); and
- whether a system of records is being created under the Privacy Act, 5 U.S.C. 552a.

Topics to cover in the PIA

- Overview
- Characterization of the information
- Uses
- Notice
- Information Sharing
- Redress
- Accountability and Security

Overview of the Program

- What does the PIA cover?
- Why are you collecting PII?
- Typical transaction
- Identify major privacy risks and ways to mitigate them

Authorities and Other Requirements

- Most straightforward section of the PIA, everything fact-based
- Legal authorities:
 - Explain how the [statutory and regulatory authority](#) permits the project and the collection of the subject information.
 - The [Privacy Act is NOT an authority](#) for collection of PII.
- Privacy Act Coverage
 - List appropriate [SORN and citation](#), check forms for appropriate e(3) statements
 - Footnote SORN citations
- Other Compliance Areas: System Security Plan, Records Retention Schedule, Paperwork Reduction Act requirements

Characterization of the Information

Applicable FIPPs:

- **Purpose Specification:**
 - Is the **information collection consistent with the program's purpose**? Does it comply with the relevant SORN and legal authorities noted in Section 1.0 for the project?
- **Data Minimization:**
 - Is the **data collected the minimum amount necessary** for the project to fulfill its mission?
 - Consider the sensitivity of each individual PII data element and the sensitivity of the combined PII data elements. An individual's SSN is more sensitive than their phone number or ZIP code.
- **Individual Participation:**
 - Collection of PII from other than the individual or from pre existing DHS records requires explanation of why the sources are preferable, relevant, and sufficiently reliable.
- **Data Quality and Integrity:**
 - Consider how accurate the information needs to be for the purposes. What are the consequences of the information being wrong or being tampered with at a later date.

Uses of the Information

- Use vs. Purpose
 - Purpose is the program or mission objective requiring the information and is directly connected to the statutory authority for the agency program.
 - Uses are the specific ways or operations (usually repetitive in nature) in which the information is processed.
- How the information is used by the Agency: Is the data queried for patterns? Is new information produced? Is there intra-agency sharing?

Uses of the Information

Applicable FIPPs:

- **Purpose Specification and Use Limitation:**
 - Is the use of information contained in the system relevant to the mission of the project?
 - As a general rule, the more regular uses made of the PII the greater will be the potential for privacy weaknesses.
 - If a system performs internal analytical functions on PII, creates internally new information about the individual, or gets data from sources other than the individual, then vulnerability may also increase.
- **Transparency:**
 - Are the PIA and SORN, if applicable, clear about the uses of the information?

Notice

- Describe how **notice** offered to individuals is **reasonable and adequate** in relation to the **system's purpose and uses**, the sensitivity of the PII, the capabilities for notice permissible within the system's design, and the limitations (e.g., Privacy Act exemptions) required by law or mission necessity.

Notice

Applicable FIPPs:

Transparency:

- Has sufficient notice been provided to the individual, including PIA or SORN?
- Do all forms have the appropriate PRA and e(3) information?

• Use Limitation:

- Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

• Individual Participation:

- Has the program provided notice to the individual of how the program provides for redress including access and correction, including other purposes of notice such as types of information and controls over security, retention, disposal, etc.?
- Does an individual have the opportunity to opt-out of the information collection?

Data Retention by the Project

- The proposed schedule should match the requirements of the Privacy Act to **keep the minimum amount of PII for the minimum amount of time**, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Data Retention by the Project

Applicable FIPPs:

- **Data Minimization:**
 - Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?
- **Data Quality and Integrity:**
 - Policies and procedures for how PII that is no longer relevant and necessary is purged.
- **Security:**
 - The longer records exist, especially in an active or semi-active status, the longer they are vulnerable to unauthorized use or exposure.

Information Sharing

- Describes what is shared EXTERNALLY, for what purpose, with whom, and when
- Applicable routine uses

Information Sharing

Applicable FIPPs:

- **Use Limitation:** Sharing PII outside of the Agency should be for a purpose compatible with the purpose for which the information was originally collected.
- **Security.** Sharing PII outside of the Agency must be transmitted securely, and the same levels of security controls and protections must be in place at the receiving agency.

Redress

- Provides information on individual access and how to correct a record about him/herself
- Describes procedures that are in place other than the Privacy Act/FOIA request route
- Informs how are individuals notified of these procedures

Redress

Applicable FIPPs:

- **Individual Participation:**

- Is the individual provided with the ability to find out whether a project maintains a record relating to him?
- If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?
- Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?

Security and Accountability

- Describe what controls determine which persons may access the system and the extent of their access, what monitoring, recording, and auditing safeguards are in place to prevent or detect unauthorized access or inappropriate usage.

Security and Accountability

Applicable FIPPs:

- **Accountability and Auditing:**

- How does the project ensure that the information is used in accordance with the stated practices in the PIA?
- What privacy training is provided to users?
- What procedures are in place to determine which users may access the information, and how is access determined?
- How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system?
- What procedures are in place other than the Privacy Act/FOIA request route?
- How are individuals notified of these procedures?



Federal Privacy Council

Federal Privacy Boot Camp

Spring 2022 Agenda

Session 4: OMB A-130, A Comprehensive Privacy Program

Title Session 4: OMB A-130, A Comprehensive Privacy Program

Date April 8, 2022 (Friday)

Location Virtual

Time 1:00 PM - 5:00 PM

Time	Topic	Presenter(s)
1:00 PM – 2:15 PM	OMB Circular A-130, M-16-24 & M-17-06	Charlie Cutshall, CFTC Kevin Herms, ED
2:15 PM – 2:30 PM	Break	
2:30 PM – 3:45 PM	Cont'd	
3:45 AM – 4:00 PM	Break	
4:00 PM – 5:00 PM	Cont'd	

Required Reading

- OMB Circular A-130, Appendix II

<https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf>

Attendance and Credit

Boot Camp staff will record attendance via the virtual platform during each session. This record will be used to determine your applicable credits at the conclusion of the training.

- The Federal Privacy Boot Camp qualifies as a training for CLP credit for federal employees. The entire camp is worth 32 credits, 4 per session over 8 sessions.
- If a session ends early, attendees that stay for the full session still earn 4 credits. Those with late arrival or early departure will have credit hours rounded up to the nearest hour.

Should you not be able to attend a session, please give Boot Camp staff advanced notice as soon as possible. If you miss more than two (2) sessions without notice, you will receive a notification that you will be dropped from the Boot Camp if you miss a third.

Session Materials

Weekly emails with slides and materials will be distributed to attendees. Materials will also be posted on the [Privacy Boot Camp MAX page](https://community.max.gov/x/ZwU1S) (<https://community.max.gov/x/ZwU1S>).

Listservs

The Privacy Boot Camp Listserv (privacy-bootcamp@listserv.gsa.gov) has been created to facilitate ongoing discussion during this program. This listserv is not actively moderated and instead will operate as an open forum for discussion. We encourage you to engage with one another through this platform to get to know your privacy peers across Government.

Please email the Privacy Council Inbox (privacy.council@gsa.gov) if you would like to be added as a subscriber to any of the following Privacy Council listservs:

- PRIVACY-COUNCIL: Broadest distribution to the Federal privacy community. Includes a bi-weekly Privacy Post newsletter. General announcements related to the FPC.
- FPC-AIC and AIC-DISCUSSION: List for the Agency Implementation Committee which hosts monthly calls that feature (1) updates from SAOP council meetings, (2) presentations, (3) guided discussions relating to privacy topics, and (4) open Q&A.
- FPC-TI-AI: List for the Artificial Intelligence Working Group within the FPC Technology and Innovation Working Group.
- PRIVACY-JOBS: Subscribers receive and are able to distribute federal privacy job announcements.

Federal Privacy Boot Camp

Session 4



Federal Privacy Council

What is a Privacy Program?

OMB Circular A-130, M-16-24, and M-17-06



**Kevin Herms &
Charlie Cutshall**



Disclaimer

- This presentation provides a general overview of recent OMB guidance on developing a comprehensive privacy program
- This presentation **does not**:
 - Provide legal advice or interpretations
 - Offer interpretations of OMB policies
 - Establish or modify any OMB policies
- Nothing in this presentation may be used or cited for any official purpose





What is a Privacy Program?

Who?

How?

What?

Huh?



What is not a Privacy Program?

An information security program is not a privacy program.

Privacy Security

“[P]rivacy and Security are independent and separate disciplines.” OMB M-16-24



Information Security

- **Information Security** means protecting information and information systems from **unauthorized** access, use, disclosure, disruption, modification, or destruction in order to provide—
 - **Integrity**: guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity;
 - **Confidentiality**: preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
 - **Availability**: ensuring timely and reliable access to and use of information.

What is not a Privacy Program?



Privacy is **not** just a check-the-box compliance exercise.



So, what is a Privacy Program?

So excited!

Tell me!

Privacy!
Privacy!
Privacy!

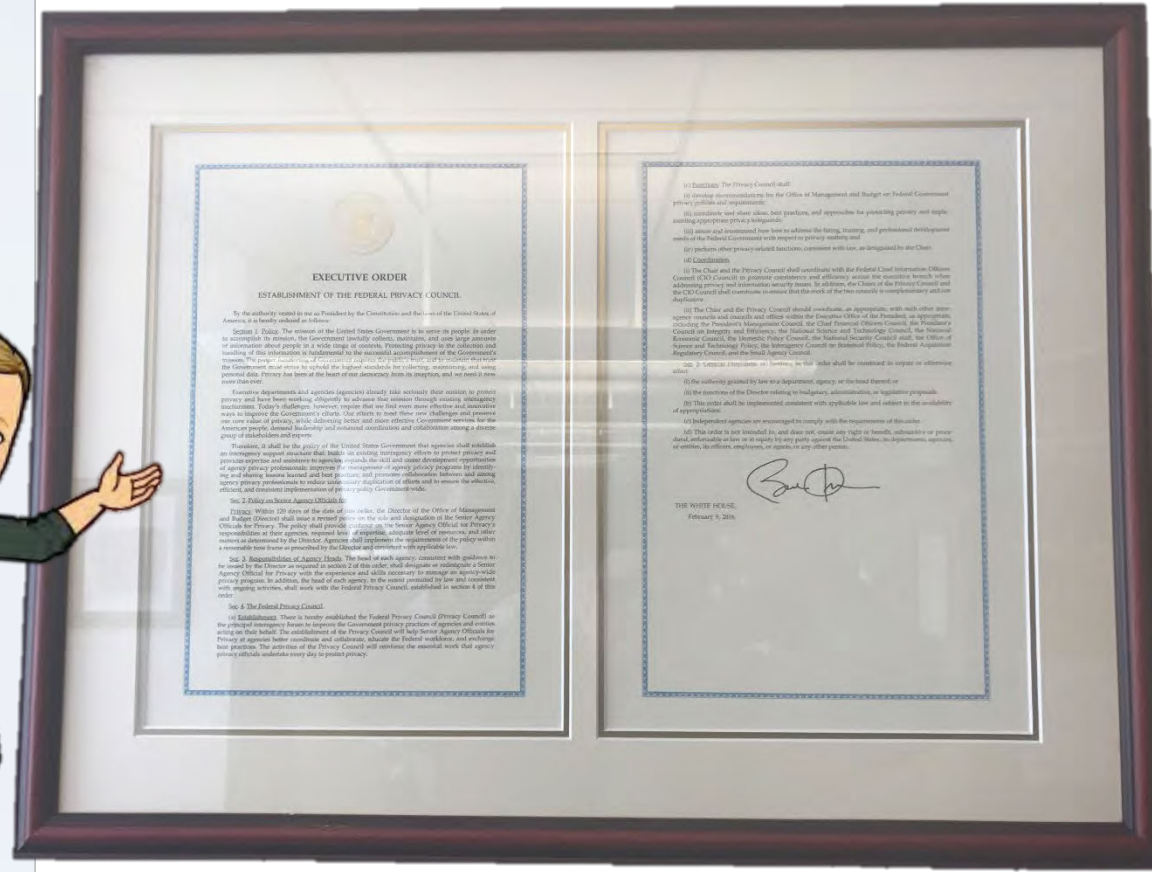


OMB Circular A-130

Federal agencies are required to establish and maintain **a comprehensive privacy program** that:

- **Ensures compliance** with applicable privacy requirements;
- Develops and evaluates **privacy policy**;
- Manages privacy risks.

Leadership – E.O. 13719



Leadership

The head of each agency, consistent with guidance to be issued by [OMB] . . . shall designate or re-designate a Senior Agency Official for Privacy with the experience and skills necessary to manage an agency-wide privacy program.

- E.O. 13719



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

September 15, 2016

M-16-24

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shaun Donovan
Director

SUBJECT: Role and Designation of Senior Agency Officials for Privacy

This Memorandum revises policies on the role and designation of the Senior Agency Official for Privacy (SAOP), as required by Executive Order 13719, *Establishment of the Federal Privacy Council*.¹ In particular, this Memorandum revises Office of Management and Budget (OMB) guidance on the SAOP's role and responsibilities in light of significant changes in law, policy, and technology that have occurred since OMB last issued guidance in this area. In addition, this Memorandum requires agencies to reassess their agency-wide privacy program and report to OMB on their implementation efforts within 60 days.

A few peas a day
will keep a
breach at bay!

OMB M-16-24

- Position.
- Expertise.
- Authority.



SAOP – Position

A senior official at the Deputy Assistant Secretary or equivalent level who:

- Serves in a **central leadership** position;
- Has **visibility** into relevant agency operations;
- Is **positioned highly** enough to regularly engage with other agency leadership, including the head of the agency.

SAOP – Expertise

Must have the necessary **skills, knowledge, and expertise** to lead and direct the agency's privacy program and carry out the privacy-related functions described in law and OMB policies.

SAOP – Authority

Must have the **necessary authority** to lead and direct the agency's privacy program and carry out the privacy-related functions described in law and OMB policies.

Responsibilities of the SAOP

The SAOP leads the agency's privacy program & is responsible for:

- Ensuring **compliance** with applicable privacy requirements;
- Developing and evaluating **privacy policy**;
- Managing **privacy risks** consistent with the agency's mission.

Ensuring Compliance

SAOP has a central role in **overseeing**, **coordinating**, and **facilitating** the agency's privacy compliance efforts. This includes compliance with law, regulation, and policy.

Ensuring Compliance

But remember...
privacy is **not** just a
check-the-box
compliance exercise!



Privacy Policy



- SAOP has a central **policy-making role**:
 - Addressing privacy implications of agency regulations & policies;
 - Leading evaluation of privacy implications of legislative proposals, testimony, & other materials.

Managing Privacy Risk

SAOP **manages privacy risks** throughout the life cycle of programs and information systems with PII.

More
on this
later!



PRIVACY
RISK



Delegation



At the discretion of the SAOP and consistent with applicable law, **other qualified agency personnel** may perform particular privacy functions that are assigned to the SAOP.

Delegation



Agencies should consider establishing privacy programs and privacy officials at **sub-agencies, components, or programs** where there is a need for privacy leadership in support of the SAOP.

CIRCULAR NO. A-130

TO THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

SUBJECT: Managing Information as a Strategic Resource

1. Introduction
2. Purpose
3. Applicability
4. Basic Considerations
5. Policy
 - a. Planning and Budgeting
 - b. Governance
 - c. Leadership and Workforce
 - d. IT Investment Management
 - e. Information Management and Access
 - f. Privacy and Information Security
 - g. Electronic Signatures
 - h. Records Management
 - i. Leveraging the Evolving Internet
6. Government-wide Responsibilities
7. Effectiveness
8. Oversight
9. Authority
10. Definitions
11. Inquiries

Circular A-130

- OMB Circular A-130, *Managing Information as a Strategic Resource* (July 28, 2016)
- The **Paperwork Reduction Act** requires OMB to “develop and oversee the implementation of uniform information resources management policies, principles, standards, and guidelines.” 44 U.S.C. § 3504(b)(1)

What is Circular A-130 about?

- A-130 provides general policy for the planning, budgeting, governance, acquisition, and management of **Federal information** as a strategic resource
- A-130 pertains to **information resources**, which can include information, information systems, technology, equipment, infrastructure, personnel, funds, etc.

Circular A-130 – Rethinking Privacy

- Elevates the role & status of the SAOP to be a **coequal partner** with her agency counterparts
- Helps agencies transition from privacy as merely a compliance exercise to privacy as a **strategic, comprehensive, continuous, risk-based** program
- Requires better coordination between privacy & security officials & more effectively integrates the SAOP into the **Risk Management Framework**

Circular A-130 – Definitions

- A-130 provides **government-wide definitions** of numerous privacy-related terms.

- 57) ‘Personally identifiable information’ means information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual.
- 58) ‘Privacy continuous monitoring’ means maintaining ongoing awareness of privacy risks and assessing privacy controls at a frequency sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.
- 59) ‘Privacy continuous monitoring program’ means an agency-wide program that implements the agency’s privacy continuous monitoring strategy and maintains ongoing awareness of threats and vulnerabilities that may pose privacy risks; monitors changes to

Circular A-130 – FIPPs

A-130 provides a set of standardized **Fair Information Practice Principles** (FIPPs) – widely accepted principles that agencies should use when evaluating systems, processes, programs, and activities affecting privacy.

When a privacy problem comes along...You must FIPP it!



Circular A-130 – Privacy Program

- Section 5 of **Appendix II** summarizes many privacy program requirements:
 - General requirements
 - Considerations for managing PII
 - Budget & acquisition
 - Contractors & third parties
 - Privacy impact assessments
 - Workforce management
 - Training & accountability
 - Incident response
 - Risk management framework

A-130 – General Requirements

General Requirements

Agencies shall have comprehensive privacy programs that ensure compliance with applicable privacy requirements, develop and evaluate privacy policy, and manage privacy risks.

- Establish and maintain a comprehensive privacy program.
- Ensure compliance with privacy requirements and manage privacy risks.
- Monitor Federal law, regulation, and policy for changes.
- Develop and maintain a privacy program plan.
- Designate a Senior Agency Official for Privacy.
- Ensure coordination between privacy and other programs.
- Ensure that privacy is addressed throughout the life cycle of each information system.
- Incorporate privacy requirements into the enterprise architecture.
- Comply with the Privacy Act.
- Conduct privacy impact assessments.
- Balance the need for information collection with privacy risks.
- Comply with requirements for disclosure and dissemination.
- Maintain and post privacy policies on websites, mobile applications, and other digital services.
- Provide performance metrics and reports.

Circular A-130 – Privacy Program

The requirements can be roughly divided into two categories:

1. **Resources of the Privacy Program**



1. **Management of PII**

PII

A-130 – Budget & Acquisition

Budget and Acquisition

Agencies' privacy programs shall have the resources needed to manage Federal information resources that involve PII. This will require privacy programs to play a key role in the development of the agencies' budget requests, as well as any decisions to acquire or develop information system technologies and services.

- Identify and plan for resources needed for privacy programs.
- Include privacy requirements in IT solicitations.
- Establish a process to evaluate privacy risks for IT investments.
- Ensure that privacy risks are addressed and costs are included in IT capital investment plans and budgetary requests.
- Ensure that investment plans meet the privacy requirements appropriate for the life cycle stage of the investment.
- Ensure that SAOP's are made aware of information systems and components that cannot be protected.





Resources of the Privacy Program

(Included in OMB M-16-24)

Agencies must identify and plan for the **financial**, **human**, **information**, and **infrastructural** resources necessary to carry out the privacy-related functions in law and OMB policies.

Resources of the Privacy Program

(Included in OMB M-16-24)

When assessing **resource needs**, agencies must consider factors such as the agency's:

- Size and structure;
- Mission, and the volume, sensitivity, and uses of PII to support the mission;
- Information resources with PII; and
- Privacy risks associated with PII.

The Most Important Resource

**Teamwork
makes the
dream work.**



A-130 – Workforce Management

Workforce Management

Agencies' privacy programs shall play a key role in workforce management activities. The SAOP shall be involved in assessing the hiring and professional development needs at the agency with respect to privacy.

- Ensure that the SAOP is involved in assessing and addressing privacy hiring, training, and professional development needs.
- Maintain a workforce planning process.
- Develop a set of privacy competency requirements.
- Ensure that the workforce has the appropriate knowledge and skill.
- Take advantage of flexible hiring authorities for specialized positions.

A-130 – Contractors & Third Parties

Contractors and Third Parties

Agencies' privacy programs shall ensure that entities that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of information on behalf of a Federal agency or that operate or use information systems on behalf of a Federal agency, comply with the privacy requirements in law and OMB policies.

- Ensure that contracts and other agreements incorporate privacy requirements.
- Maintain agency-wide privacy training for all employees and contractors.
- Ensure that the Privacy Act applies to contractors where required.
- Oversee information systems operated by contractors.
- Implement policies on privacy oversight of contractors.
- Ensure implementation of privacy controls for contractor information systems.
- Maintain an inventory of contractor information systems.
- Ensure that incident response procedures are in place for contractor information systems.



A-130 – Training & Accountability

Training and Accountability

Agencies' privacy programs shall develop, maintain, and provide agency-wide privacy awareness and training programs for all employees and contractors. In addition, the privacy program shall establish rules of behavior for employees and contractors with access to PII and hold agency personnel accountable for complying with applicable privacy requirements and managing privacy risks.

- Maintain agency-wide privacy training for all employees and contractors.
- Ensure that privacy training is consistent with applicable policies.
- Apprise agency employees about available privacy resources.
- Provide foundational and advanced privacy training.
- Provide role-based privacy training to appropriate employees and contractors.
- Hold personnel accountable for complying with privacy requirements and policies.
- Establish rules of behavior for employees and contractors with access to PII and consequences for violating the rules.
- Ensure that employees and contractors read and agree to rules of behavior.



A-130 – Considerations for PII

Considerations for Managing PII

Agencies' privacy programs shall maintain an inventory of PII, regularly review all PII maintained by the agency, and comply with applicable requirements regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII. In addition, agencies' privacy programs shall impose, where appropriate, conditions on other agencies and entities to which PII is being disclosed that govern the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of the PII.

- Maintain an inventory of agency information systems that involve PII and regularly review and reduce PII to the minimum necessary.
- Eliminate unnecessary collection, maintenance, and use of Social Security Numbers.
- Follow approved records retention schedules for records with PII.
- Limit the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.
- Require entities with which PII is shared to maintain the PII in an information system with a particular categorization level.
- Impose conditions on the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of shared PII through agreements.

A-130 – Privacy Impact Assessments

Privacy Impact Assessments

Agencies shall conduct a privacy impact assessment (PIA) under section 208(b) of the E-Government Act of 2002, absent an applicable exception under that section, when the agency develops, procures, or uses information technology to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.

- Analyze how PII is handled to ensure that handling conforms to applicable privacy requirements, to determine the privacy risks associated with an information system or activity, and to evaluate ways to mitigate privacy risks.
- Conduct and draft a PIA with sufficient clarity and specificity to demonstrate that the agency fully considered privacy and incorporated appropriate privacy protections from the earliest stages of the agency activity and throughout the information life cycle.
- Update PIAs whenever changes to the information technology, changes to the agency's practices, or other factors alter the privacy risks associated with the use of such information technology.
- Post on the agency's website, unless doing so would raise security concerns or reveal classified or sensitive information.

A-130 – Incident Response

Incident Response

Agencies' privacy programs shall develop and implement incident management and response capabilities.

- Maintain formal incident management and response policies and capabilities.
- Establish roles and responsibilities to ensure oversight and coordination of incident response.
- Periodically test incident response procedures.
- Document incident response lessons learned and update procedures.
- Ensure that processes are in place to verify corrective actions.
- Report incidents in accordance with OMB guidance.
- Provide reports on incidents as required.

A-130 – Risk Management Framework

Risk Management Framework

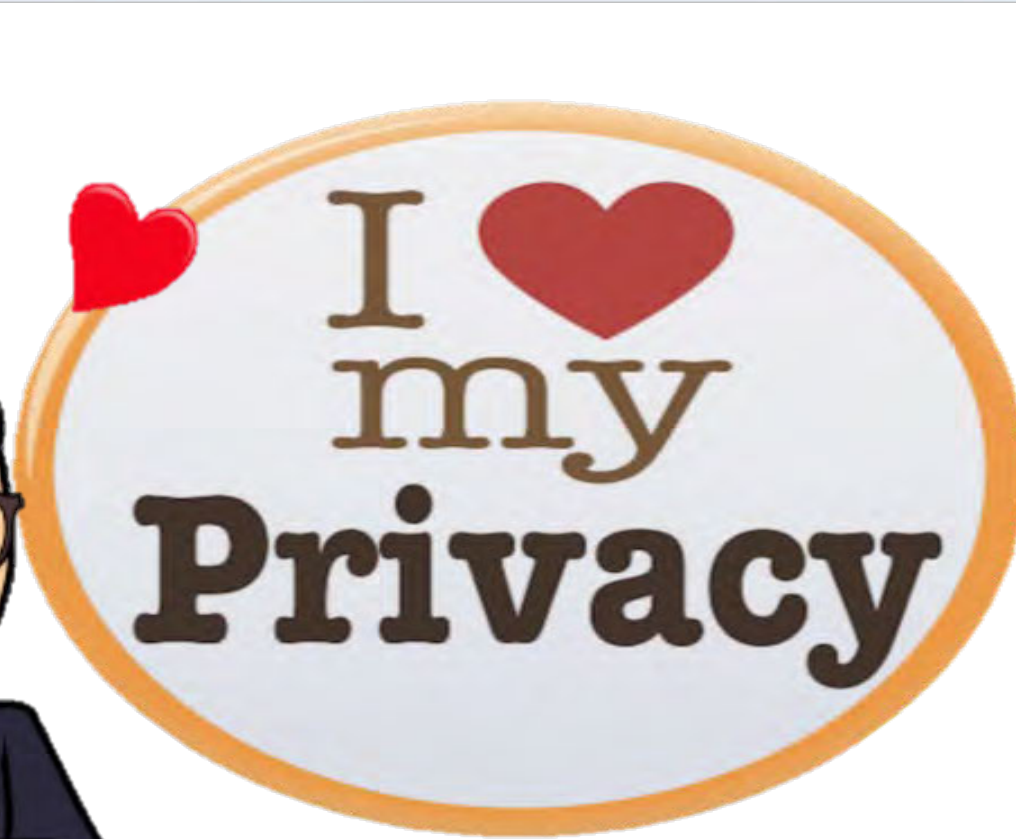
Agencies' privacy programs have responsibilities under the Risk Management Framework. The Risk Management Framework provides a disciplined and structured process that integrates information security, privacy, and risk management activities into the information system development life cycle.

- Implement a risk management framework.
- Review and approve the categorization of information systems that involve PII.
- Designate program management, common, information system-specific, and hybrid privacy controls.
- Implement a privacy control selection process.
- Develop, approve, and maintain privacy plans for information systems.
- Identify privacy control assessment methodologies and metrics.
- Conduct assessments of privacy controls.
- Correct deficiencies that are identified in information systems.
- Develop and maintain a privacy continuous monitoring strategy.
- Establish and maintain a privacy continuous monitoring program.
- Review authorization packages for information systems that involve PII.

Understanding Privacy and the Risk Management Framework



Kevin Herms
Charlie Cutshall



CIRCULAR NO. A-130

TO THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

SUBJECT: Managing Information as a Strategic Resource

1. Introduction
2. Purpose
3. Applicability
4. Basic Considerations
5. Policy
 - a. Planning and Budgeting
 - b. Governance
 - c. Leadership and Workforce
 - d. IT Investment Management
 - e. Information Management and Access
 - f. Privacy and Information Security
 - g. Electronic Signatures
 - h. Records Management
 - i. Leveraging the Evolving Internet
6. Government-wide Responsibilities
7. Effectiveness
8. Oversight
9. Authority
10. Definitions
11. Inquiries



Privacy Goals of New A-130

- Elevates the role & status of the SAOP to be a **coequal partner** with her counterparts at the agency.
- Helps agencies transition from privacy as merely a compliance exercise to privacy as a **strategic, comprehensive, continuous, risk-based** program.
- Requires better coordination between privacy & security officials & more effectively integrates the SAOP into the **Risk Management Framework**.

What is the RMF?

- The RMF provides a disciplined & structured process that **integrates privacy**, information security, & risk management activities into the **information system development life cycle**.
- Effectively implementing the RMF ensures that agencies appropriately manage information system-related risks consistent with the agency's **mission** and **risk tolerance**.

What is an information system?

- Federal agencies are principally concerned with managing the risk to **information** and **information system**.
- Privacy requirements apply to personally identifiable information in **any form or medium**, including paper and electronic media.
- Information systems may include but are not limited to information technology systems.



- An “information system” is a discrete set of **information resources** organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. § 3502).
- ‘Information resources’ means information and related resources, such as **personnel, equipment, funds,** and **information technology** (44 U.S.C. § 3502).

What is “Privacy Risk”?

- FISMA is about “**information security**,” which includes “**confidentiality**.”
- However, the RMF requires agencies to manage privacy risks **beyond** those that are typically included under the heading of “confidentiality.”



What is “Privacy Risk”?

- Privacy risks can involve unauthorized access or disclosure of PII – but they can also result from other activities, including:
 - **creation, collection, use, & retention** of PII;
 - inadequate **quality** or **integrity** of PII; and
 - lack of appropriate **notice, transparency, or participation.**

Privacy & the RMF

- **Privacy control** – an administrative, technical, or physical safeguard employed within an agency to ensure compliance with applicable privacy requirements & manage privacy risks.
- The SAOP shall **designate** which privacy controls will be treated as:
 - common controls;
 - information system-specific controls;
 - hybrid controls; and
 - program management controls.

Privacy & the RMF



Program Management Controls

Privacy & the RMF

- **Program management control** – a privacy control that is generally implemented at the agency level, independent of any particular information system, & essential for managing an agency's privacy program.
- Program management controls shall be documented in the agency's **privacy program plan**.

Program Management Controls

Privacy & the RMF

- The **privacy program plan** provides an overview of the agency's privacy program, including:
 - a description of the **structure** of the privacy program;
 - the **resources** dedicated to the privacy program;
 - the **role of the SAOP** and other privacy officials and staff;
 - the **strategic goals & objectives** of the privacy program;
 - the **program management controls** & **common controls** in place or planned; and
 - any other information determined necessary by the agency's privacy program.

Program Management Controls

Privacy & the RMF



Privacy & the RMF



Prepare

Organization Tasks:

- Identify and assign key roles
- Develop a Risk Management Strategy
- Identify Common Controls
- Continuous Monitoring Strategy

Privacy & the RMF



Prepare

Information-system Level Tasks:

- Identify the authorization boundary
- Identify the information life cycle
- Conduct risk assessments
- Define privacy requirements

Privacy & the RMF



Categorize

- SAOP shall **review** and **approve** the categorization of information systems that involve PII.
- Information systems are categorized at **low**, **moderate**, or **high** based on the impact of a potential loss of confidentiality, integrity, or availability

Privacy & the RMF



Select

- Agencies shall employ a process to **select** privacy controls for information systems.
- Agencies shall develop & maintain a **privacy plan** that documents the privacy controls selected for an **information system**, how the controls have been implemented, & the metrics that will be used to assess the controls.

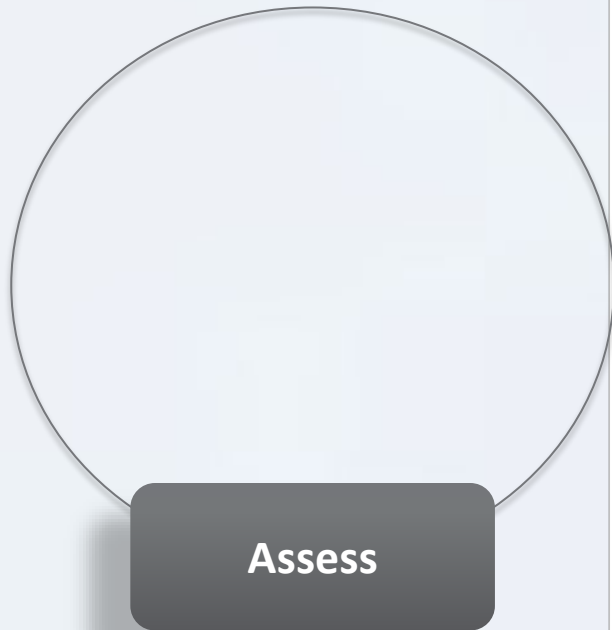
Privacy & the RMF



Implement

- Agencies shall employ a process to **implement** privacy controls selected for information systems and shall document how the controls are implemented in the system's **privacy plan**.

Privacy & the RMF



- SAOP shall conduct and document **privacy control assessments** to ensure that privacy controls are implemented correctly & operating as intended.
- SAOP shall identify assessment **methodologies & metrics**.
- Agencies shall correct **deficiencies** identified through privacy control assessments.

Privacy & the RMF

- SAOP shall review **authorization packages** for information systems that involve PII.
- Authorization packages include the system security plan, privacy plan, security & privacy control assessment, & any POA&Ms.



Authorize

Privacy & the RMF

- Agencies shall monitor & assess selected privacy controls on an **ongoing basis**.
- The ongoing assessment of privacy controls & privacy risks is referred to as **privacy continuous monitoring (PCM)**.



Monitor

Privacy & the RMF



Monitor

- SAOP shall develop & maintain a written **PCM strategy** that catalogs the available privacy controls.
- SAOP shall assign an **assessment frequency** to each privacy control that is sufficient to ensure compliance with applicable privacy requirements & manage privacy risks.

Privacy & the RMF

- SAOP shall establish & maintain a **PCM program** to implement the PCM strategy.
- The PCM program is an agency-wide program that is responsible for:
 - **maintaining ongoing awareness** of threats & vulnerabilities that may pose privacy risks;
 - **monitoring changes** to information systems & environments of operation;
 - conducting privacy control **assessments**.



Monitor

Privacy & the RMF



Program Management Controls

Questions?



Policies for Public Websites and Digital Services



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

November 8, 2016

M-17-06

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shaun Donovan
Director, Office of Management and Budget
Howard Shelanski H.S.
Administrator, Office of Information and Regulatory Affairs
Tony Scott
Federal Chief Information Officer

SUBJECT: Policies for Federal Agency Public Websites and Digital Services

Federal Agency public websites and digital services are the primary means by which the public receives information from and interacts with the Federal Government. These websites and services help the public apply for benefits, search for jobs, comply with Federal rules, obtain authoritative information, and much more. Federal websites and digital services should always meet and maintain high standards of effectiveness and usability and provide quality information that is readily accessible to all.



OMB M-17-06

- OMB Memorandum M-17-06, *Policies for Federal Agency Public Websites and Digital Services* (Nov. 8, 2016)
- M-17-06 provides agencies with guidance on public-facing websites and other digital services, which are the primary means by which the public receives information about the government.

Transparency

- One of the FIPPs standardized in A-130 is **transparency** – agencies should be transparent about their privacy practices.
- Each agency must maintain a **Privacy Program Page** at the URL [agency].gov/privacy dedicated to the agency's privacy program.

Privacy Program Page

- Complete, up-to-date versions of system of records notices (SORNs)
- Privacy impact assessment (PIAs)
- Matching notices & agreements
- Exemptions to the Privacy Act
- Privacy Act implementation rules
- Publicly available agency privacy policies
- Publicly available agency privacy reports
- Instructions for submitting a Privacy Act request
- Contact information for submitting a question or complaint
- Contact information for the SAOP



Home » About DOJ

Office of Privacy and Civil Liberties Home

▼ About the Office

Frequently Asked Questions

▼ Privacy Act of 1974

Overview

DOJ System of Records Notices

DOJ Computer Matching Agreements

DOJ Privacy Act Regulations

Judicial Redress Act of 2015

▼ E-Government Act of 2002

DOJ Privacy Impact Assessments

Privacy Compliance Process

Resources

Reports

Career Opportunities

Training Opportunities

OPCL FOIA

Contact the Office

OFFICE OF PRIVACY AND CIVIL LIBERTIES



MISSION

The Office of Privacy and Civil Liberties (OPCL) supports the duties and responsibilities of the Department's Chief Privacy and Civil Liberties Officer (CPCLO). The principal mission of OPCL is to protect the privacy and civil liberties of the American people through review, oversight, and coordination of the Department's privacy operations. OPCL provides legal advice and guidance to Departmental components; ensures the Department's privacy compliance, including compliance with the Privacy Act of 1974, the privacy provisions of both the E-Government Act of 2002 and the Federal Information Security Modernization Act of 2014, as well as administration policy directives issued in furtherance of those Acts; develops and provides Departmental privacy training; assists the CPCLO in developing Departmental privacy policy; prepares privacy-related reporting to the President and Congress; and reviews the information handling practices of the Department to ensure that such practices are consistent with the protection of privacy and civil liberties.

GENERAL INFORMATION OFFICE OF PRIVACY AND CIVIL LIBERTIES

LEADERSHIP

Peter A. Winn
Director, Office of Privacy and Civil Liberties

CONTACT

Office of Privacy and Civil Liberties
privacy@usdoj.gov



Questions?





Federal Privacy Council

Federal Privacy Boot Camp

Spring 2022 Agenda

Session 5: Privacy Breaches & Identity Theft

Title Session 5: Privacy Breaches & Identity Theft

Date April 22, 2022 (Friday)

Location Virtual

Time 1:00 PM - 5:00 PM

Time	Topic	Presenter(s)
1:00 PM – 2:15 PM	Breaches	Brooke Dickson, DOE (b) (7)(C), USCG
2:15 PM – 2:30 PM	Break	
2:30 PM – 3:30 PM	Breaches Cont'd	
3:30 pM – 3:45 PM	Break	
3:45 PM – 5:00 PM	Identity Theft	Kelle Slaughter, FTC

Suggested Reading

- Data Breach Guidance M-17-12:
https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf
- FAR Contracts Language:
 - FAR 24.104
 - 52.224-1 Privacy Act Notification
 - 52.224-2 Privacy Act
 - 27.404-4 Contractor's release, publication, and use of data
 - 27.404-6 Inspection of data at the contractor's facility

Attendance and Credit

Boot Camp staff will record attendance via the virtual platform during each session. This record will be used to determine your applicable credits at the conclusion of the training.

- The Federal Privacy Boot Camp qualifies as a training for CLP credit for federal employees. The entire camp is worth 32 credits, 4 per session over 8 sessions.
- If a session ends early, attendees that stay for the full session still earn 4 credits. Those with late arrival or early departure will have credit hours rounded up to the nearest hour.

Should you not be able to attend a session, please give Boot Camp staff advanced notice as soon as possible. If you miss more than two (2) sessions without notice, you will receive a notification that you will be dropped from the Boot Camp if you miss a third.

Session Materials

Weekly emails with slides and materials will be distributed to attendees. Materials will also be posted on the [Privacy Boot Camp MAX page](https://community.max.gov/x/ZwU1S) (<https://community.max.gov/x/ZwU1S>).

Listservs

The Privacy Boot Camp Listserv (privacy-bootcamp@listserv.gsa.gov) has been created to facilitate ongoing discussion during this program. This listserv is not actively moderated and instead will operate as an open forum for discussion. We encourage you to engage with one another through this platform to get to know your privacy peers across Government.

Please email the Privacy Council Inbox (privacy.council@gsa.gov) if you would like to be added as a subscriber to any of the following Privacy Council listservs:

- PRIVACY-COUNCIL: Broadest distribution to the Federal privacy community. Includes a bi-weekly Privacy Post newsletter. General announcements related to the FPC.
- FPC-AIC and AIC-DISCUSSION: List for the Agency Implementation Committee which hosts monthly calls that feature (1) updates from SAOP council meetings, (2) presentations, (3) guided discussions relating to privacy topics, and (4) open Q&A.
- FPC-TI-AI: List for the Artificial Intelligence Working Group within the FPC Technology and Innovation Working Group.
- PRIVACY-JOBS: Subscribers receive and are able to distribute federal privacy job announcements.

Federal Privacy Boot Camp

Week 5



Federal Privacy Council

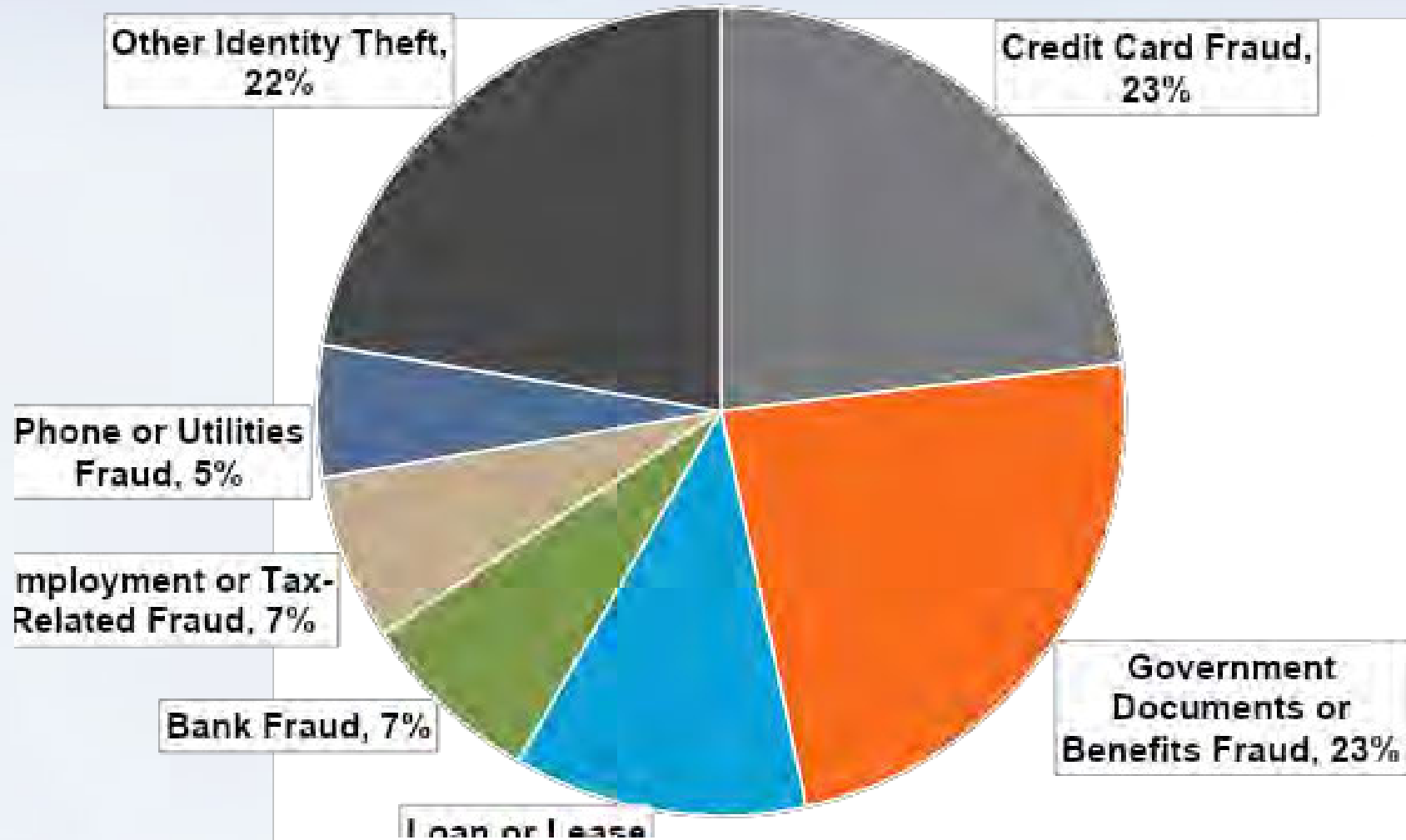
Understanding Identity Theft

Scope of the Problem

January – December 2021

1.4
million reports

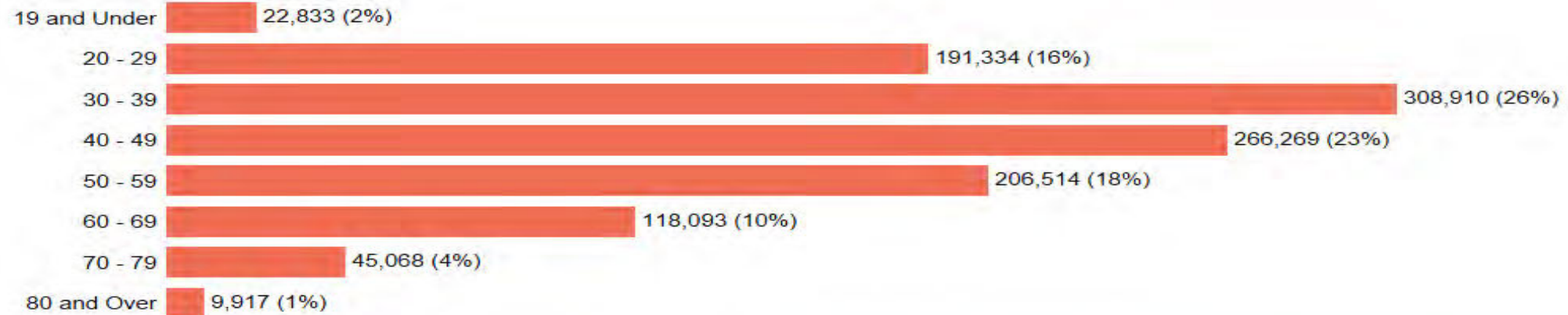
2021 FTC Identity Theft Reports



Identity Theft by Age

Year: 2021

Identity Theft Reports by Age



Identity Theft Types by Age

Theft Type	19 and Under	20 - 29	30 - 39	40 - 49	50 - 59	60 - 69	70 - 79	80 and Over
Bank Fraud	1,664	15,333	25,802	25,461	23,795	17,647	7,580	1,961
Credit Card Fraud	1,707	65,269	108,592	76,693	45,741	21,992	7,507	1,954
Employment or Tax-Related Fraud	14,578	21,697	25,027	17,967	13,845	8,824	3,882	1,502
Government Documents or Benefits Fraud	2,467	15,873	32,390	65,693	77,270	49,094	19,153	3,038
Loan or Lease Fraud	1,003	41,239	65,163	41,855	21,936	9,105	2,465	505
Other Identity Theft	2,722	61,910	103,283	74,288	43,581	20,072	6,981	1,710
Phone or Utilities Fraud	696	20,134	27,161	17,330	10,069	5,026	1,839	457

Of the 1,434,676 total identity theft reports in 2021, 81% included consumer age information.

Ways Identity Theft Can Happen

Offline

- Lost or stolen wallet or smart phone
- Theft by friends or family
- Stolen mail
- Dumpster diving
- Corrupt insider

Online

- Phishing
- Smishing
- Skimming
- Shimming
- Data breaches
- Imposter scams

Government Benefits Fraud

What is it?

When imposters file a claim for unemployment insurance, using your name and personal information.



Government Benefits Fraud

What to do. . .

- Report the government benefits identity theft to the state benefits office where it occurred
- Consider a fraud alert or a credit freeze
- Continue to monitor your credit report



Credit Card Fraud

What is it?

Credit card fraud is the unauthorized use of a credit or debit card to fraudulently obtain money or property.



Credit Card Fraud

What to do. . .

- Use ATMs inside bank (or pay the cashier at gas stations), when possible.
- Cover the keypad when entering your PIN.
- Use credit not debit, when possible.
- Watch statements carefully. Report anything suspicious ASAP.



Synthetic Identity Theft

What is it?

A form of identity theft in which criminals combine pieces of real personal data with fake information to create an entirely new identity, one that's almost impossible to detect.



Synthetic Identity Theft

What to do. . .

- Be vigilant. Guard your Social Security number.
- Monitor your credit report. Get your free credit report: AnnualCreditReport.com.
- Consider a credit freeze for you and your family.
- Suspect identity theft? Take action at IdentityTheft.gov

Video



Romance Scams

What is it?

- You meet someone on a dating website or social media platform
- They want to email or talk by phone
- They say they love or deeply care about you but they need money for a plane ticket to visit or for an emergency
- They ask you to wire money, load a gift card, or invest in cryptocurrency

Romance Scams

What to do. . .

- Don't send money or gift cards or cryptocurrency investments
- Don't share sensitive information
- Research the person
- Report Romance Scams at [ReportFraud.gov](https://reportfraud.gov)
- For more information about imposter scams, go to ftc.gov/imposters



Avoiding Identity Theft

Reducing the Risk of Identity Theft Offline

- Guard your Social Security number
- Shred financial documents
- Don't share personal info when someone asks
- Keep your info safe at home
- Check the mail as soon as you can
- Monitor your accounts and financial statements
- Get your free credit report: AnnualCreditReport.com
- Consider a credit freeze



Reducing the Risk of Identity Theft Online

- Use strong passwords
- Use multifactor authentication
- Keep your security software up to date
- Keep your operating system updated, too
- Don't click links in emails or texts that come out of the blue
- Before you pay: is your connection secure?

Video



Get your FREE Annual Credit Report

- Visit annualcreditreport.com or call 1-877-322-8228.
 - Or complete the [Annual Credit Report Request Form](#) and mail it.
- You may order from each of the **three** nationwide credit reporting companies at the same time, or stagger them.
- You are entitled to one free copy from each of the nationwide credit reporting companies every 12 months. Due to the pandemic, you can get free weekly credit reports through December 2022.



Reviewing Credit Reports

Red Flags

- Incorrect name, address, SSN, and employer information
- Unknown accounts
- Unknown charges on current accounts
- High volume of inquiries from companies you have not contacted

Action Steps

- Review your report from each credit bureau
- Contact them to fix any mistakes (Learn more: [ftc.gov/credit](https://www.ftc.gov/credit))
- Suspect identity theft? Take action at [IdentityTheft.gov](https://www.IdentityTheft.gov)

Recovery and Mitigating Risks

Fraud Alerts & Credit Freezes

Fraud Alerts & Credit Freezes: What's the Difference?

Looking for ways to protect your identity?
Here are two options to consider.



Fraud Alert

- ✓ Makes lenders verify your identity before granting new credit in your name. (Usually, they'll call you to verify your identity.)
- ✓ Free
- ✓ Available to anyone who is or suspects they may be affected by identity theft
- ✓ Lasts one year
- ✓ To place: Contact **one** of the three credit bureaus. That bureau must tell the other two.

Credit Freeze

- ✓ Restricts access to your credit report to help prevent identity theft. (Usually, you'll need a PIN or password to place or lift the freeze.)
- ✓ Free
- ✓ Available to anyone
- ✓ Lasts until you lift it
- ✓ To place or lift: Contact **all three** credit bureaus. (If you know which bureau a lender will use, you can lift for only that one.)

IdentityTheft.gov

The screenshot shows the IdentityTheft.gov website. At the top, the Federal Trade Commission logo and the text 'FEDERAL TRADE COMMISSION IdentityTheft.gov' are visible. There are 'Log in' and 'En Español' links in the top right. The main heading reads 'Report identity theft and get a recovery plan' with a large 'Get Started' button featuring a right-pointing arrow. Below this is a link that says 'or browse recovery steps'. A section titled 'IdentityTheft.gov can help you report and recover from identity theft. HERE'S HOW IT WORKS:' follows. It contains a three-step process: 1. 'Tell us what happened.' with a speech bubble icon and text explaining that users will be asked questions about their situation. 2. 'Get a recovery plan.' with a 'TO DO:' list icon and text explaining that a personal recovery plan will be created. 3. 'Put your plan into action.' with a 'TO DO:' list icon showing checkmarks and text explaining that users will be guided through recovery steps, can update their plan, track progress, and receive pre-filled forms and letters.

FEDERAL TRADE COMMISSION
IdentityTheft.gov

Log in En Español

Report identity theft and get a recovery plan

Get Started →

or browse recovery steps

IdentityTheft.gov can help you report and recover from identity theft.
HERE'S HOW IT WORKS:

Tell us what happened.
We'll ask some questions about your situation. Tell us as much as you can.

Get a recovery plan.
We'll use that info to create a personal recovery plan.

Put your plan into action.
If you create an account, we'll walk you through each recovery step, update your plan as needed, track your progress, and pre-fill forms and letters for you.



IdentityTheft.gov



COMISIÓN FEDERAL DE COMERCIO

Robo de Identidad.gov

One-stop Resource

- Streamlined process to report and recover
- Personal recovery plans for more than 30 types of identity theft
- Online consumer guidance
- Create an Identity Theft Report
- Customized sample letters
- Reports shared with other law enforcement agencies



FEDERAL TRADE COMMISSION

Identity Theft Report

FTC Report Number:
101055143

I am a victim of Identity theft. This is my official statement about the crime.

Contact Information

First Name:		Last Name:	
Average		Consumer	
Address:	Phone:	Email:	
123 Main St. Muskegon , MI 49510 USA	202-441-4183	joyrop@hotmail.com	

Personal Statement

I recently got a large credit card bill for a card I did not open. When I called Bank of America, they said someone opened up an account using all of my information. I am worried they will open more accounts and how to clear this debt as well.

Accounts Affected by the Crime

Credit Card Opened by the Thief		
Company or Organization: Bank of America		
Account Number: 9999 9999 9999 9999		
Date fraud began:	Date that I discovered it:	Total fraudulent amount:
1/2022	12/2021	\$ 56893

Under penalty of perjury, I declare this information is true and correct to the best of my knowledge.

I understand that knowingly making any false statements to the government may violate federal, state, or local criminal statutes, and may result in a fine, imprisonment, or both.

Average Consumer
Average Consumer1/14/2022
Date

Use this form to prove to businesses and credit bureaus that you have submitted an FTC Identity Theft Report to law enforcement. Some businesses might request that you also file a report with your local police.





FEDERAL TRADE COMMISSION

IdentityTheft.gov

Log In

En Español

Your Report is not submitted yet.

Almost Done! We recommend creating a **free account** so you can:

- Get a **personal recovery plan** that tracks your progress
- Print **prefilled** letters & forms
- Return anytime to **update and view** your affidavit
- **Save time** if this ever happens again

Yes, submit and create account →

No thanks, submit without an account

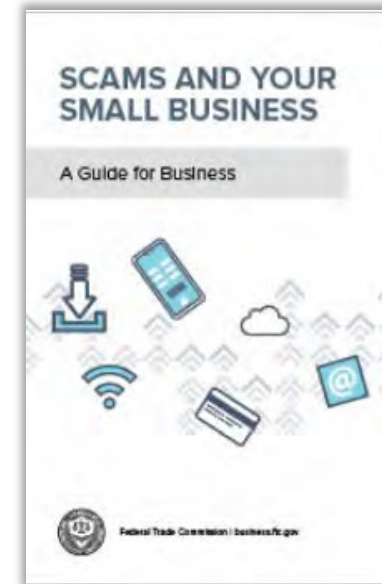
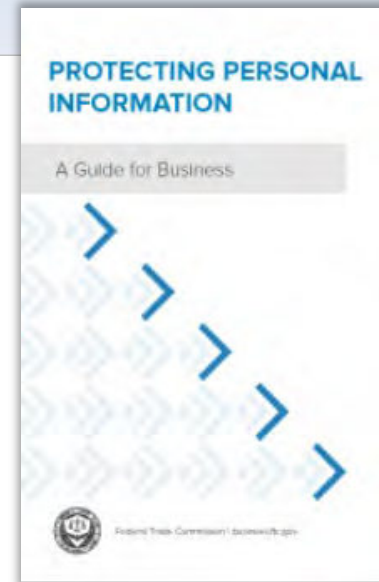
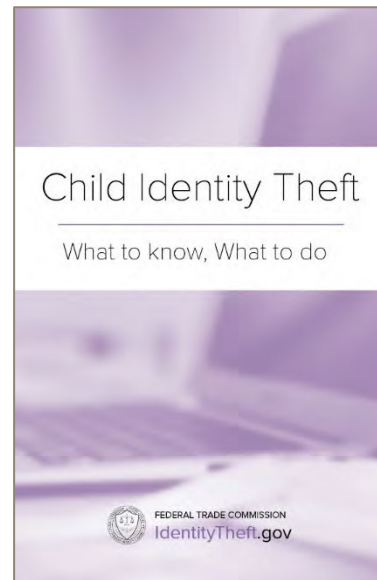
I understand that I will **NOT** be able to make updates.

Instead, I will receive a **one-time copy** of my affidavit and recovery plan.

IdentityTheft.gov Video



Resources



Order FREE publications: [ftc.gov/bulkorder](https://www.ftc.gov/bulkorder)



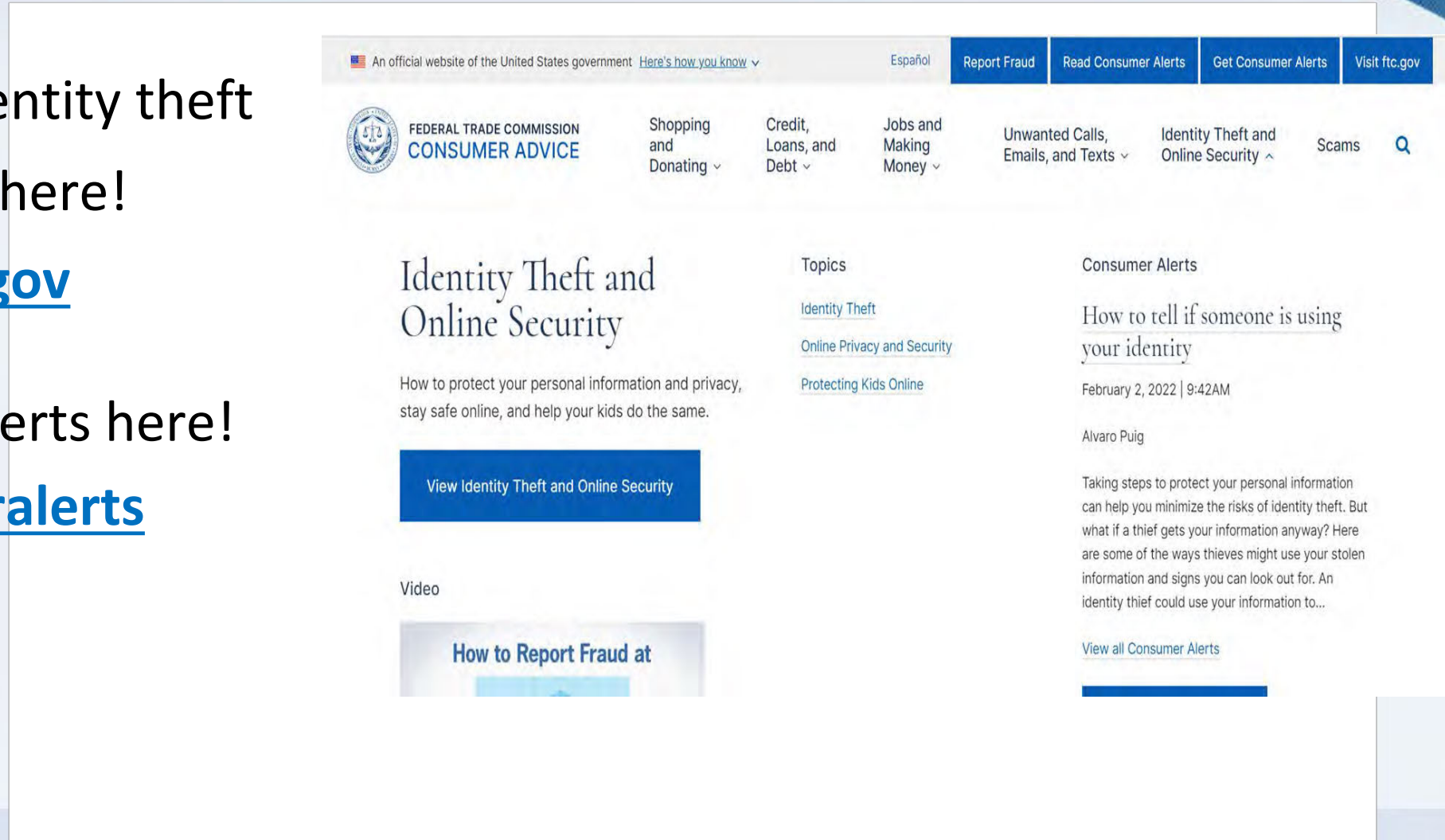
Other Resources

Learn how to avoid identity theft
and other scams here!

consumer.ftc.gov

Get your consumer alerts here!

ftc.gov/consumeralerts



The screenshot displays the Federal Trade Commission's Consumer Advice website. At the top, there is a navigation bar with links for "Report Fraud", "Read Consumer Alerts", "Get Consumer Alerts", and "Visit ftc.gov". Below this, the main header includes the FTC logo and the text "FEDERAL TRADE COMMISSION CONSUMER ADVICE". A secondary navigation bar lists various topics: "Shopping and Donating", "Credit, Loans, and Debt", "Jobs and Making Money", "Unwanted Calls, Emails, and Texts", "Identity Theft and Online Security", and "Scams". The main content area is titled "Identity Theft and Online Security" and includes a sub-header "How to protect your personal information and privacy, stay safe online, and help your kids do the same." A prominent blue button labeled "View Identity Theft and Online Security" is visible. To the right, there is a "Topics" section with links for "Identity Theft", "Online Privacy and Security", and "Protecting Kids Online". Further right, a "Consumer Alerts" section features an article titled "How to tell if someone is using your identity" dated February 2, 2022, by Alvaro Puig. The article text discusses minimizing the risks of identity theft and mentions that thieves might use stolen information and signs to look out for. A "View all Consumer Alerts" link is provided at the bottom of the article. A "Video" section is partially visible at the bottom left, showing a thumbnail for "How to Report Fraud at".





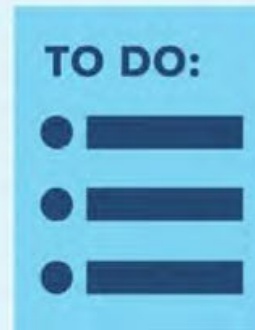
FEDERAL TRADE COMMISSION
ReportFraud.ftc.gov

Start your report now

ReportFraud.ftc.gov



Tell us what happened



Get next steps



Help stop fraud

SPANISH: ReporteFraude.ftc.gov



Thank you!

Federal Privacy Boot Camp

Session 5



Federal Privacy Council

No two breaches are the same.....

Similar circumstance can have different outcomes.

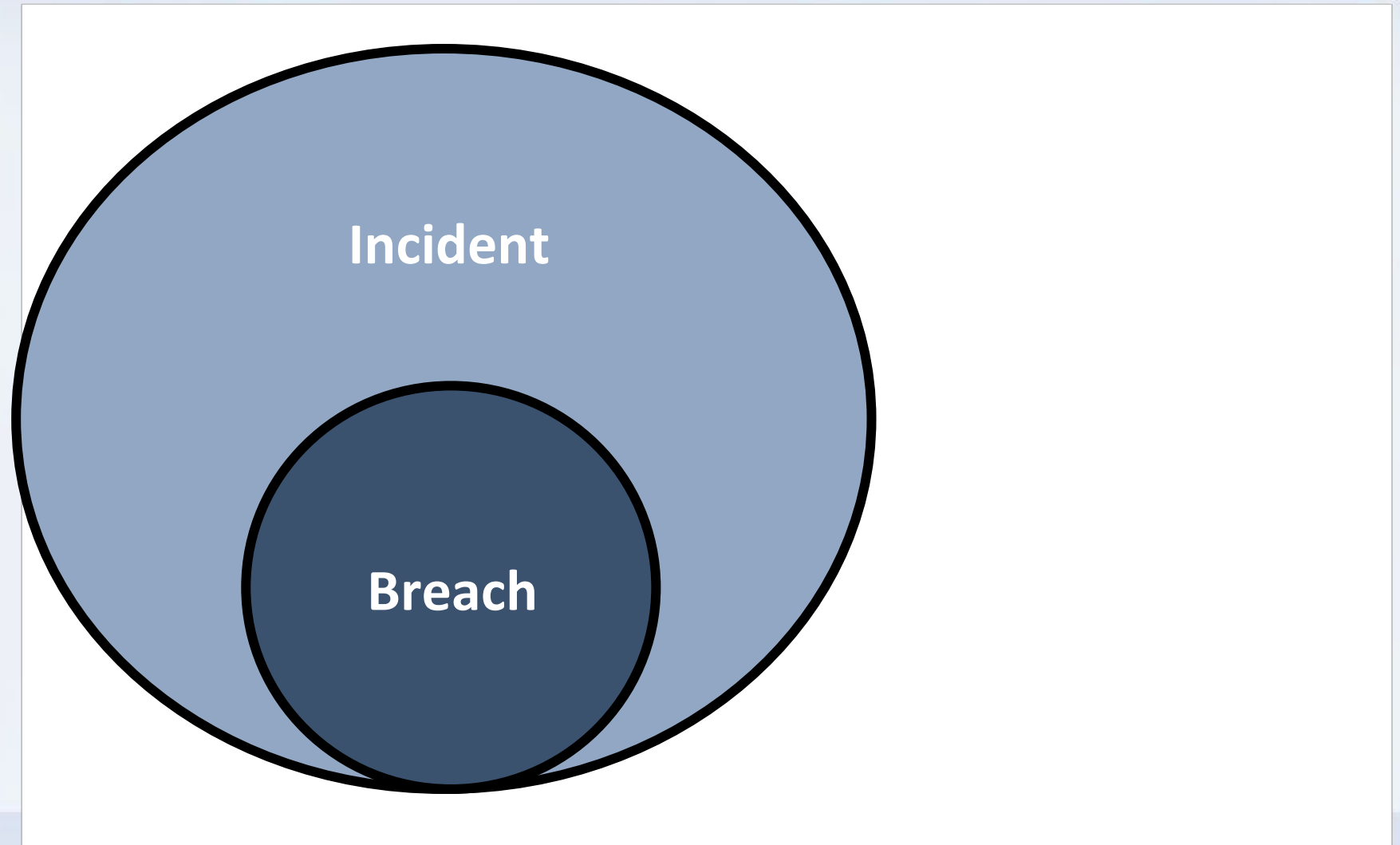
Everyone has been affected by a data breach at some point...

....but you may not be aware that your PII was exposed.

Key Concepts



Visual Definition



Definitions

- **Incident**: An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.”
- **Breach**: The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose.

Test Your Knowledge #1

- An employee at government agency XYZ leaves a bag with her agency-issued laptop and 20 resumes, including SF-50s, in the backseat of her car. Upon returning to her car, she realizes that the laptop bag has been stolen.
- Breach? Incident? Neither?

Test Your Knowledge #2

- An employee at government agency XYZ, who is on the procurement team, is surfing through his organization's SharePoint site and discovers a folder titled "EEO Actions." He decides to open the folder and, surprised that he has access, spends the remainder of his day reading EEO actions filed by other XYZ employees across the agency.
- Breach? Incident? Neither?

Test Your Knowledge #3

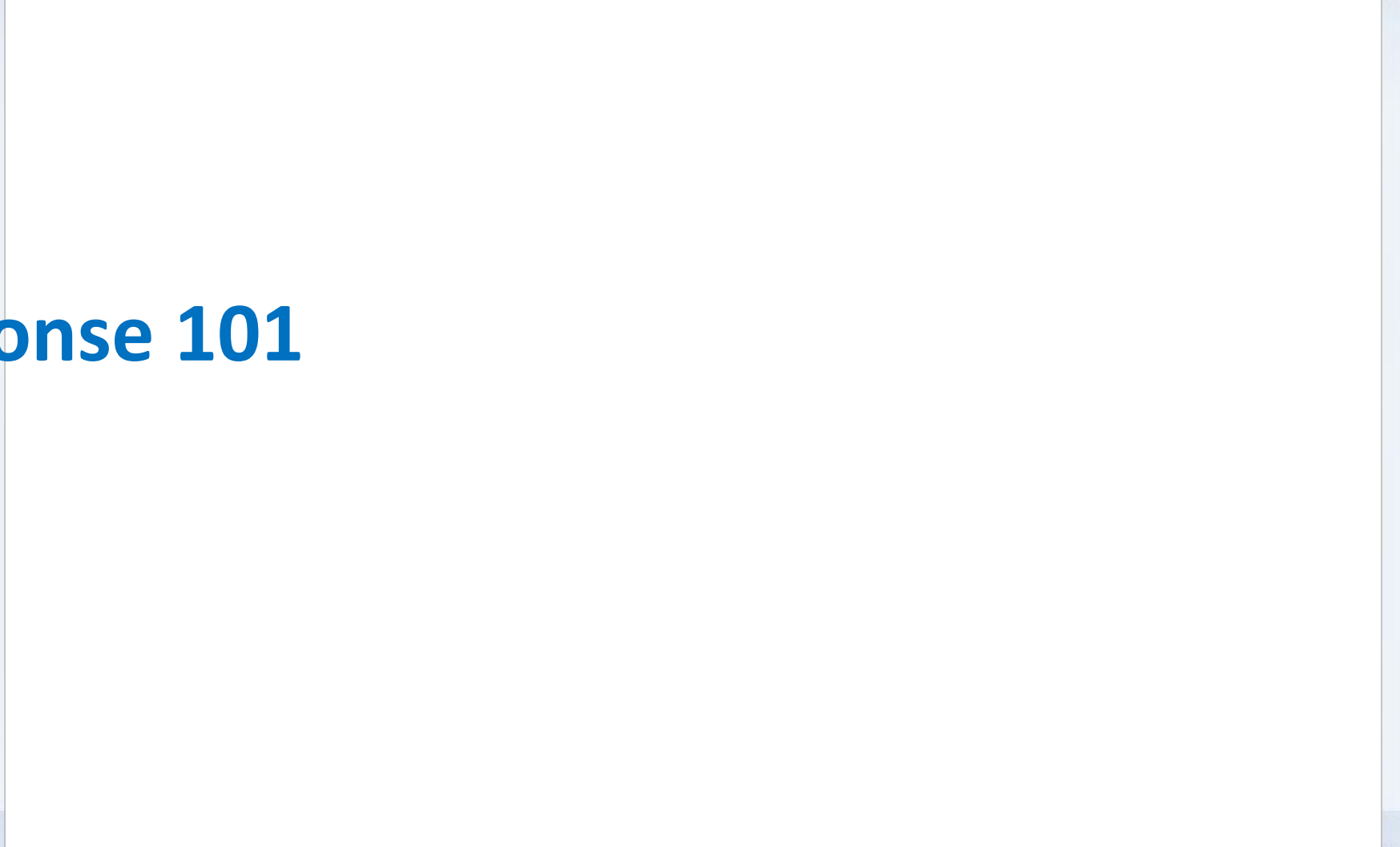
- An employee at government agency XYZ is thrilled to receive an email alerting him that he has won the lottery. To access his winnings, he follows the email instructions and clicks on a link to receive his prize. Six days later, his mouse cursor starts moving on its own.
- Breach? Incident? Neither?

Test Your Knowledge #4

- An employee sends his tax W-2 form from his government email address to his personal email address. He hits Send and realizes that his W-2 included his Social Security number and was sent unencrypted.
- Breach? Incident? Neither?

Questions about Test your Knowledge?

Breach Response 101



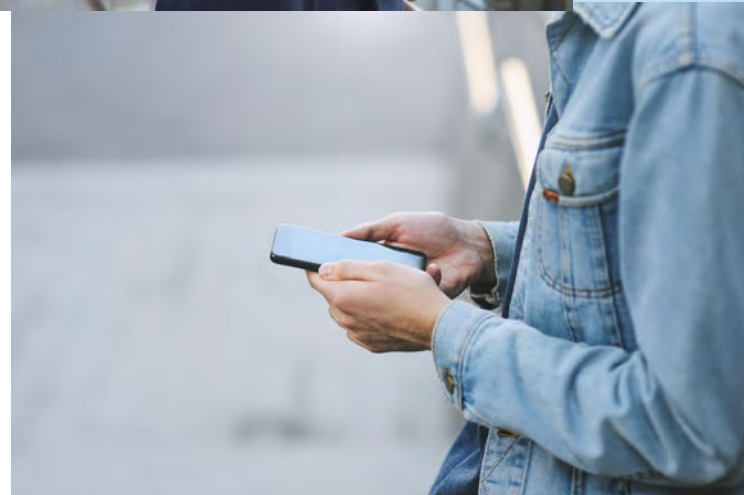
In the Beginning....

- *Since 2005, millions of federal records have been lost or compromised by data breaches.*
- OMB established privacy breach response framework and guidance including:
 - OMB M-06-15, *Safeguarding Personally Identifiable Information* (May 22, 2006);
 - OMB M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments* (July 12, 2006);
 - Recommendations for Identity Theft Related Data Breach Notification (Sept. 20, 2006); and
 - OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007).

Level Setting

- Incidents and Breaches come in a variety of flavors...
 - Simple:
 - Physical mail gets delivered to the wrong person;
 - An email was sent to the wrong person within the same agency.
 - Complex:
 - Loss of data integrity or system access affects multiple components and mission activities of an agency;
 - A database is compromised;
 - Poorly configured permission allow unauthorized access to sensitive data;
 - Ransomware attack.

Where Breaches Occur



Breaches by the Numbers

- Human error continues to be #1 cause
- Unencrypted emails continue to be the #1 medium
- SSNs continue to be the #1 PII element
- Financial Information is the #1 most harmful loss

The Principles of PII Breach Response

- Policies, procedures, and practices
- Breach reporting and tracking
- Identification and investigation of breach
- Assessing the risk of harm to individuals
- Mitigating the risk of harm to individuals
- Notifying individuals and other protection services
- Closeout reporting
- Training and awareness

Cyber vs Privacy Outcomes

While cybersecurity and privacy work together to investigate reported incidents and breaches, each group has different interests and target outcomes.

- **Cybersecurity** wants to ensure that **threats** are mitigated to IT networks, systems, or entry points into the agency's IT infrastructure.
- **Privacy** wants to ensure that **individuals** do not face harm as a result of the breach of PII.

PII Breaches and Federal Agencies

- The US Government collects exponential amounts of information about people: its employees, members of the public, visitors to the U.S., and others.
 - Agencies need PII to fulfill mission and business needs.
 - Agencies have a responsibility to safeguard any information it collects, and to respond appropriately if it mishandles that information.
- When an agency loses information, it can lead to a series of potential harms, including identity theft, embarrassment, and loss of trust/reputation.

Preparation is the First Step...



Be Prepared: Breach Response Plan

- Each agency must develop a Breach Response Plan formalizing agency policies and procedures for reporting, investigating, and managing a breach.
- The Breach Response Plan should be tailored to the agency and address the agency's mission, size, structure, and functions.
- The Plan should also account for different responses depending on type of breach
- The plan should complement cyber response plans and practices

Components of an Agency Breach Response Plan

The Breach Response Plan should address:

- The agency's Breach Response Team
- Technical support from Cyber/SOC when remediating a breach
- Identifying applicable privacy compliance documentation
- Information sharing to respond to a breach
- Reporting requirements
- Assessing the risk of harm to individuals potentially affected by a breach
- Mitigation of the risk of harm
- Notification
- Closure

Is it time to panic?

- Plans should account for thresholds and circumstances. Not everything is five alarms:



Sending your tax W-2s from work email to your own personal email.



Documents with PII left unattended in an agency cafeteria for 30 minutes.



Unencrypted security files for multiple individuals accidentally sent to a group email list or organizational distribution list and opened by dozen of recipients.

Be Prepared: Setting Up Your Breach Response Team

- The agency's Breach Response Team (BRT) is a group of officials designated by the head of the agency that the Senior Agency Official for Privacy (SAOP) may convene to respond to a breach.
- Agency BRT should include, at a minimum:
 - The SAOP
 - The Chief Information Officer (CIO) or the CIO's designee
 - The Senior Agency Information Security Officer
 - Legal counsel
 - Legislative affairs
 - Public Affairs
 - Program Office/System Owner of system or data included in breach

REMINDER! Not every breach requires a BRT.....

Who Reports to Whom?

Understand your SOC's reporting process

- Methods for Initial report intake
- Distribution to experts for follow-up action
- Reporting and communications
 - Internal
 - External
 - White House/Congress
- Maintaining and updating reports
- Keeping stakeholders informed of developments

The Basics: Breach Reporting Requirements

- Employees and contractors must report suspected or confirmed incidents and breaches to agency SOC.
- Agencies must report all incidents and breaches involving PII to the NCCIC/US-CERT at DHS Cybersecurity and Infrastructure Reporting Agency (CISA) according to the requirements in the NCCIC/US-CERT Federal Incident Notification Requirements. Generally done by the SOC. Breaches must be reported within ONE hour of discovery.
- NCCIC/US-CERT will assign a tracking number in addition to your agency's internal SOC tracking number. Keep both numbers handy.

Reporting Requirements: Major Incident

- A “major incident” is “any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American People.”
- A breach is a major incident when it involves PII that “if exfiltrated, modified, deleted, or otherwise compromised” results in...
 - demonstrable harm to the national security interests, foreign relations, or economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people [*REGARDLESS OF NUMBER OF INDIVIDUALS*] and/or
 - 100,000 potentially impacted individuals.
- Agencies must report to CISA and OMB within one hour of determining a major incident occurred.

Training and Awareness

- Training and Awareness is critical to ensuring that incidents and breaches are reported within ONE hour of discovery.
- Agency breach response processes, including reporting contact information, should be part of the agency's annual Privacy Act and Privacy Awareness Training.
- Use awareness events, such as National Cybersecurity Awareness Month, to remind employees and contractors of their reporting responsibilities!

10 minute break!!



Game Plan: The Steps of Breach Response



The Steps of Breach Response



Breach Response Starts Here

- Rules of Behavior
- NIST security and privacy controls
- Government employees
- Contractors
 - Federal Acquisition Regulations (FAR)
 - Privacy Act clauses
 - Incident reporting clauses
 - PII breach clauses
 - DFARSs/Agency specific ARs
 - Statement of Work

Identify a Breach

- Identification
 - Is this PII?
 - Does it involve information in different formats (paper, electronic, verbal)?
 - How many individuals are potentially affected?
 - How was the information breached?
 - Internal
 - External
 - Initial numbers of affected individuals?

Report the Breach: Internal Reporting

- Suspected or Confirmed
 - Agency reporting process
 - Local level
 - “...to the agency as soon as possible and without unreasonable delay....”
- Mechanics of reporting
 - Up to the agency and within the organization

.... And then to NCCIC/US-CERT.

Report the Breach: Questionable Circumstances

- Non-reportable breach examples
 - Own PII after a determination is made through investigation
 - Normally releasable: office / rolodex PII (OPM: 5 CFR 293.311)
 - Unencrypted email; need to know; within the firewall [some agencies require encryption/password-protection internally]
 - ISSM confirmed DoD approved DAR encryption

Investigation and Response to Breach

Track

- Assign tracking number
- Acknowledge breach

Classify & Investigate

- Location of breach?
- Initial Investigation
- Major Incident?
- Other stakeholders to involve or make aware?

Assess

- Conduct a risk analysis
 - OMB M-17-12
- PII element classification
 - Sensitive PII?
 - NIST SP 800-122 (Apr 2010)

Privacy Team vs. Security Team

- Privacy and Security teams should work together when investigating and responding to a breach, but each have differing roles in the process:
 - **Security**: focused on technical and security remediation, including forensics.
 - **Privacy**: focused on identifying types of PII; determining risk of harm; and instituting a plan for how to mitigating harm to individual.

Report the Breach: Additional Reporting

- Additional reporting

- Law enforcement
- Congress
 - NLT 7 days “...a reasonable basis to conclude that a breach constitutes a ‘major breach’ has occurred.”
 - “supplemental.....NLT 30 days after the agency discovers the breach.”
- White House/OMB

- Additional support

- Inspector General
- General Counsel

To Convene your Breach Response Team or Not...

- The agency SAOP determines whether the agency Breach Response Team (BRT) needs to be convened.
- BRTs need to prioritize breach response while convened.
- Some BRTs may want to be informed but not convened. SAOP makes the call on how to proceed.

Respond to Breach: Notification

- Make a Plan for Notification
 - What information needs to be included in the notice?
 - Who signs the notice?
 - Can notice be provided to all individual or is broader notice needed?
 - How quickly should notice be provided?
 - Is there any reason to delay notice (i.e., law enforcement investigation)?
 - How to disseminate notice [physical mail, email, public notice; media outreach]?
 - Do you have the addresses to mail notices? Is further information needed?

NOTE: Always coordinate with Public Affairs and/or Congressional Affairs

Other Forms of Response

- Identity Protection Services (IPS) [aka Credit Monitoring Services]
 - Options exist to cover individuals to large groups
 - One government plan – GSA offers blanket purchase agreement
- Things to keep in mind when offering IPS
 - Should be tied to risk analysis of harm
 - Covered individuals have to Opt-in (not automatic)
 - Only about 20% of individuals take IPS
 - Congress can mandate extension of coverage (OPM 2015)

Other Factors to Response

- Jurisdiction Overlap
 - Employees or Records of another federal agency
 - Internal component or bureau
 - State data breach laws – rare but does happen
- Federal records vs contractor-owned records
- Violations of agency policy or rules of behavior

The Financial Realities of Breach

- The Costs of Breach Response
 - Mail – materials, postage, tracking
 - Media announcements
 - Call center management
 - Identity Protection Services
 - Forensic services
 - Contractor surge support
 - Technical remediation of systems or networks (external breaches)

Other Harms Related to the Breach...

- Embarrassment
 - Individual
 - Agency
- Emotional harm
- Reputational harm
- Risk to personal safety
- Loss of benefit(s)
- Inconvenience
- Unfairness
- Loss of Trust

Close Breach

- Notifications made
- Cause corrected or prevented
- Lessons Learned
- Close within your agency tracking system
- Breach documentation
 - This should be treated as an auditable record
- BRT notes and decisions (if convened)

Ongoing Breach Related Activities

- Annual review of Agency Breach Response Plan
- FISMA annual reporting
- BRT tabletop exercises
- NIST SP 800-53 Security and Privacy Controls

It's time to apply your new knowledge!



EXERCISE: PII Breach Scenarios

- It fell off the truck...
- Ghost Writing
- Mistaken Account Identity

It fell off the truck...

An employee of agency ABC prepares multiple packages of medical documents to be shipped to site MNO via tracked mail.

Three days later, site MNO contacts the agency employee to say the shipment did not arrive.

The mail carrier investigates and discovers the driver had an accident that damaged the truck but no lost packages were reported.

Ghost Writing

A member of the acquisition department was assigned to review a database of government credit card spending and report any irregularities to the office manager.

The reviewer found that some numbers changed in the documents when she re-accessed previously viewed files. The reviewer claims that she did not make changes to the database.

During a regular audit of the organization's credit card operations, a series of version updates to various financial databases were identified. The author behind these edits is unknown and the auditor cannot trace the edits back to an identifiable agency IT user account.

Another Account by the Same Name

Agency JKL uses a cloud based file storage platform. The cloud vendor has business/government customers but members of the public can set up individual personal accounts using the service.

An employee who is going on official travel next week wants easy access to his work files while he is away from his work laptop. Some of the files include the employee's own PII but there could be other PII in the files. He knows that he cannot put the files on a removable media device (i.e., thumb drive). He discovers that he can access his personal cloud account from his work laptop and uploads several agency files into his personal file drive.

After his official travel, the employee transfers to another agency. Six months later, he discovers the work files from the previous agency on his personal cloud account. He decides to send the files to his email address at the new agency.

References

- NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations, Revision 5 (September 2020). <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>
- NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (April 2010). <https://csrc.nist.gov/publications/detail/sp/800-122/final>
- OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, (January 2017). <https://www.whitehouse.gov/omb/information-regulatory-affairs/privacy/>
- US-CERT, “US-CERT Federal Incident Notification Guidelines,” (April 2019). <https://www.us-cert.gov/incident-notification-guidelines>



Federal Privacy Council

Federal Privacy Boot Camp

Spring 2022 Agenda

Session 6: IT Security for Privacy Professionals

Title Session 6: IT Security for Privacy Professionals

Date April 29, 2022 (Friday)

Location Virtual

Time 1:00 PM - 5:00 PM

Time	Topic	Presenter(s)
1:00 PM – 2:15 PM	IT Security	Claire Barrett, NIST (b) (6), NGA
2:15 PM – 2:30 PM	Break	
2:30 PM – 3:15 PM	Cont'd	
3:15 AM – 3:30 PM	Break	
3:30 PM – 5:00 PM	Emerging Technology	Marcela Souaya, CFTC Richard Speidel

Suggested Reading

- [SP 800-53 Website](#)
- [SP 800-53r5](#), Security and Privacy Controls for Information Systems and Organizations
- [SP 800-53B](#) - Control Baselines for Information Systems and Organizations

Attendance and Credit

Boot Camp staff will record attendance via the virtual platform during each session. This record will be used to determine your applicable credits at the conclusion of the training.

- The Federal Privacy Boot Camp qualifies as a training for CLP credit for federal employees. The entire camp is worth 32 credits, 4 per session over 8 sessions.
- If a session ends early, attendees that stay for the full session still earn 4 credits. Those with late arrival or early departure will have credit hours rounded up to the nearest hour.

Should you not be able to attend a session, please give Boot Camp staff advanced notice as soon as possible. If you miss more than two (2) sessions without notice, you will receive a notification that you will be dropped from the Boot Camp if you miss a third.

Session Materials

Weekly emails with slides and materials will be distributed to attendees. Materials will also be posted on the [Privacy Boot Camp MAX page](https://community.max.gov/x/ZwU1S) (<https://community.max.gov/x/ZwU1S>).

Listservs

The Privacy Boot Camp Listserv (privacy-bootcamp@listserv.gsa.gov) has been created to facilitate ongoing discussion during this program. This listserv is not actively moderated and instead will operate as an open forum for discussion. We encourage you to engage with one another through this platform to get to know your privacy peers across Government.

Please email the Privacy Council Inbox (privacy.council@gsa.gov) if you would like to be added as a subscriber to any of the following Privacy Council listservs:

- PRIVACY-COUNCIL: Broadest distribution to the Federal privacy community. Includes a bi-weekly Privacy Post newsletter. General announcements related to the FPC.
- FPC-AIC and AIC-DISCUSSION: List for the Agency Implementation Committee which hosts monthly calls that feature (1) updates from SAOP council meetings, (2) presentations, (3) guided discussions relating to privacy topics, and (4) open Q&A.
- FPC-TI-AI: List for the Artificial Intelligence Working Group within the FPC Technology and Innovation Working Group.
- PRIVACY-JOBS: Subscribers receive and are able to distribute federal privacy job announcements.

Federal Privacy Boot Camp

**Session #6: IT Security for Privacy
Professionals**



Federal Privacy Council

Goals

- Provide overview of the Risk Management Framework (RMF)
- Provide practical guidance to successfully complete the RMF
- Develop an understanding of how Privacy converges with IT Security (Exercise)

Integrating Privacy & Security Processes

RISK MANAGEMENT FRAMEWORK

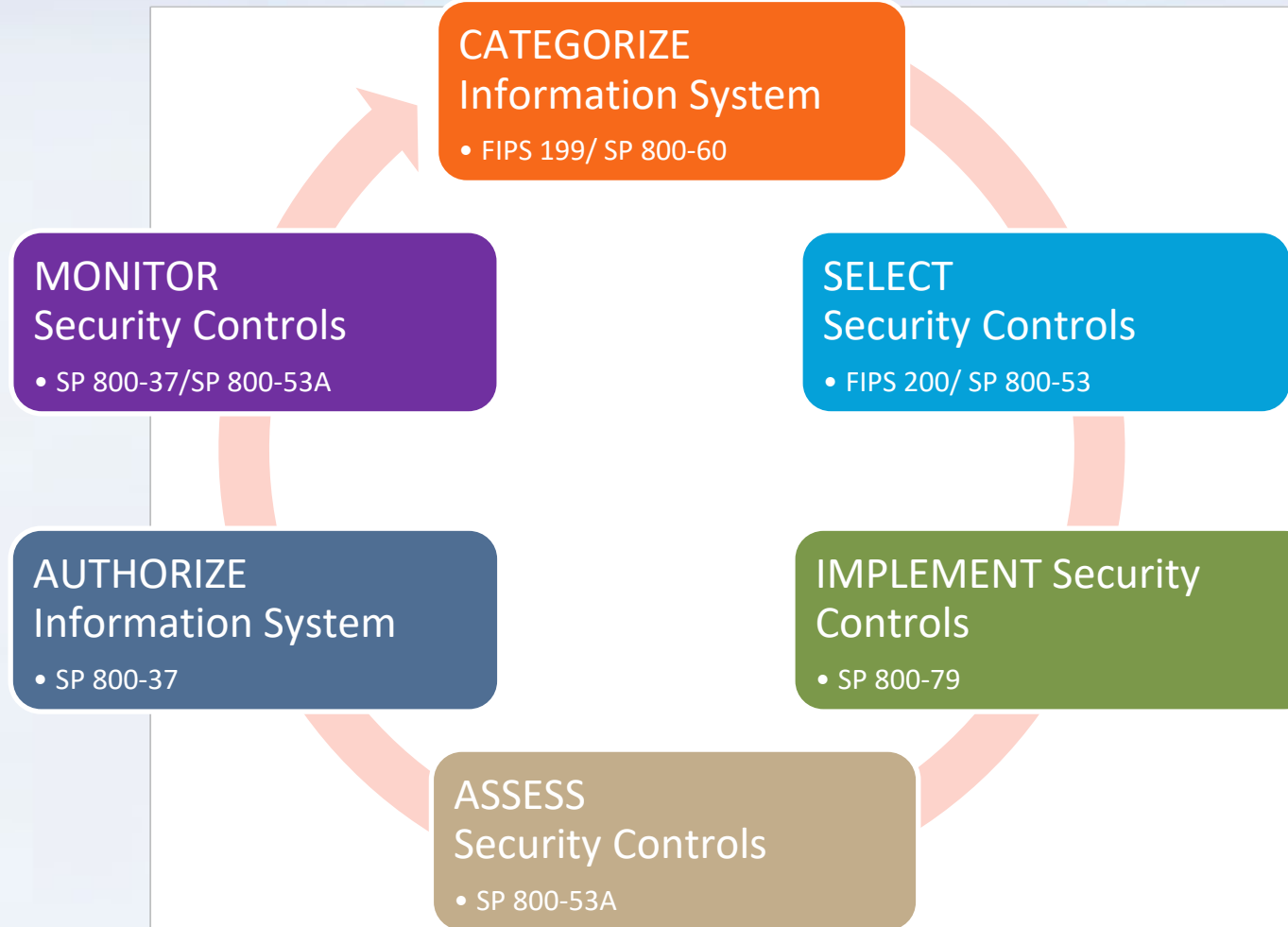


Risk Management Concepts

- Threat
- Vulnerability
- Risk
- Countermeasure / Safeguard
- Residual Risk
- Acceptable Risk

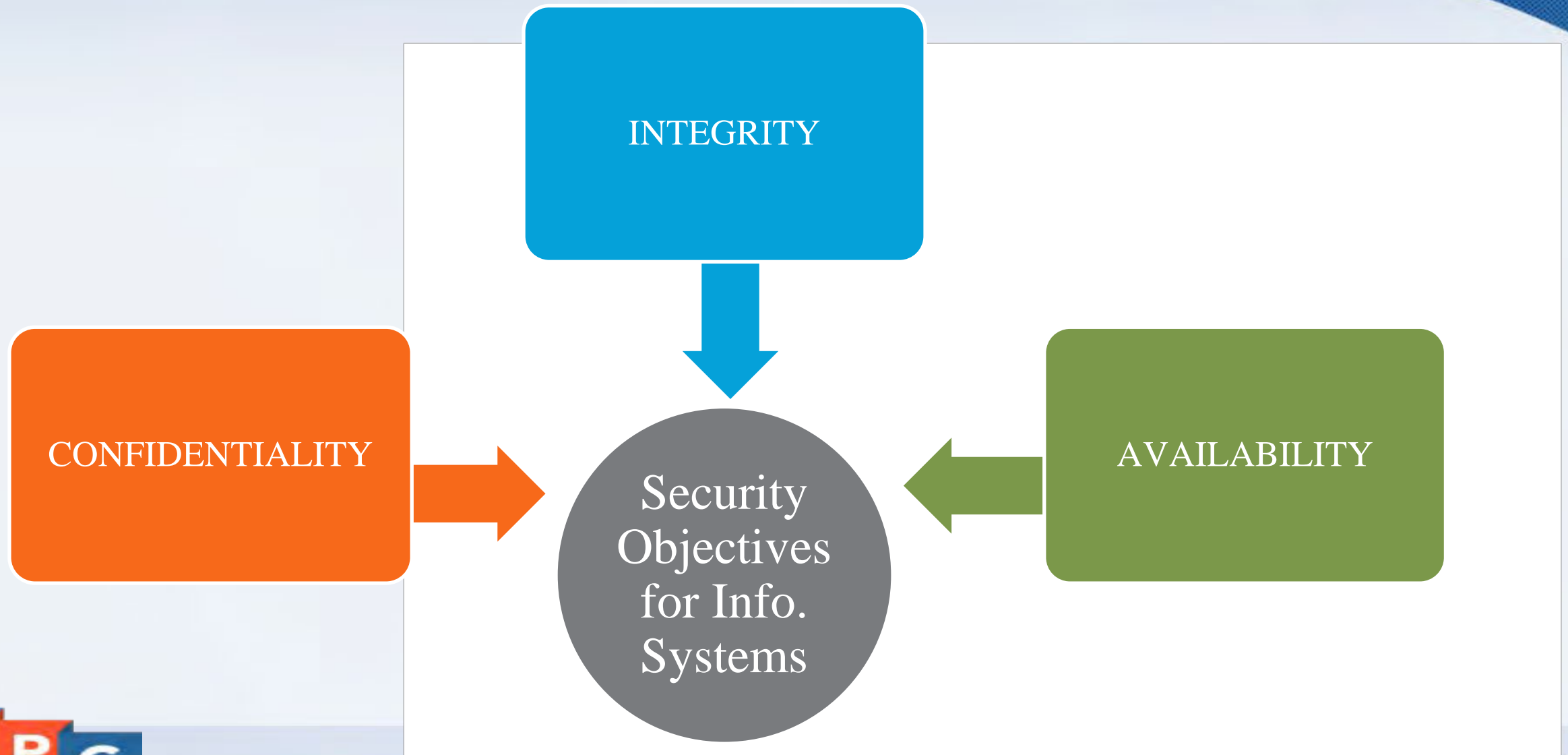
Who is responsible for
“acceptance of risk”?

Risk Management Framework



<http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/>

Security Trifecta



Security Trifecta

CONFIDENTIALITY

A loss of confidentiality is the unauthorized disclosure of information.

INTEGRITY

A loss of integrity is the unauthorized modification or destruction of information.

AVAILABILITY

A loss of availability is the disruption of access to or use of information or an information system.

FEDERAL INFORMATION PROCESSING STANDARDS (FIPS) PUBLICATION 199
Standards for Security Categorization of Federal Information and Information Systems



Security Trifecta

Security Objective	POTENTIAL IMPACT		
	LOW	MODERATE	HIGH
Confidentiality	The unauthorized <u>disclosure</u> of information could be expected to have a <u>limited</u> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized <u>disclosure</u> of information could be expected to have a <u>serious</u> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized <u>disclosure</u> of information could be expected to have a <u>severe or catastrophic</u> adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The unauthorized <u>modification or destruction</u> of information could be expected to have a <u>limited</u> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized <u>modification or destruction</u> of information could be expected to have a <u>serious</u> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized <u>modification or destruction</u> of information could be expected to have a <u>severe or catastrophic</u> adverse effect on organizational operations, organizational assets, or individuals.
Availability	The <u>disruption of access to or use</u> of information or an information system could be expected to have a <u>limited</u> adverse effect on organizational operations, organizational assets, or individuals.	The <u>disruption of access to or use</u> of information or an information system could be expected to have a <u>serious</u> adverse effect on organizational operations, organizational assets, or individuals.	The <u>disruption of access to or use</u> of information or an information system could be expected to have a <u>severe or catastrophic</u> adverse effect on organizational operations, organizational assets, or individuals.

Recent History of NIST SP 800-53

Rev 3

- Security
- One privacy control: PL-5 (Do a PIA)

Rev 4

- Security
- FIPPs-based Privacy controls in Appendix J

Rev 5

- Consolidated Security and Privacy controls and specific “PII Processing and Transparency” Control Family

What are Privacy Controls

- Structured set of privacy controls that are based on Fair Information Practice Principles (FIPPs)
- Tool to support managing organization privacy risk and compliance
- Privacy built into entire lifecycle of personally identifiable information (PII) (paper or electronic)
- Closer cooperation between privacy and security officials
- Comprehensive source of privacy requirements and implementation guidance



App. J Privacy Controls Defined

ID	Privacy Controls
AP	Authority & Purpose
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	Accountability, Audit, & Risk Management
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-6	Privacy Reporting
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	Data Quality & Integrity
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Review Board
DM	Data Minimization
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	Individual Participation and Redress
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	Security
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	Transparency
TR-1	Privacy Notice
TR-2	System of Records Notice and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	Use Limitation
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

FIPPs = Privacy Controls

Privacy Controls = FIPPs



NIST SP 800-53 Rev 5 Controls

TABLE 1: SECURITY AND PRIVACY CONTROL FAMILIES

ID	FAMILY	ID	FAMILY
<u>AC</u>	Access Control	<u>PE</u>	Physical and Environmental Protection
<u>AT</u>	Awareness and Training	<u>PL</u>	Planning
<u>AU</u>	Audit and Accountability	<u>PM</u>	Program Management
<u>CA</u>	Assessment, Authorization, and Monitoring	<u>PS</u>	Personnel Security
<u>CM</u>	Configuration Management	<u>PT</u>	PII Processing and Transparency
<u>CP</u>	Contingency Planning	<u>RA</u>	Risk Assessment
<u>IA</u>	Identification and Authentication	<u>SA</u>	System and Services Acquisition
<u>IR</u>	Incident Response	<u>SC</u>	System and Communications Protection
<u>MA</u>	Maintenance	<u>SI</u>	System and Information Integrity
<u>MP</u>	Media Protection	<u>SR</u>	Supply Chain Risk Management

PII Processing and Transparency (PT) Control Family

TABLE C-15: PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY FAMILY

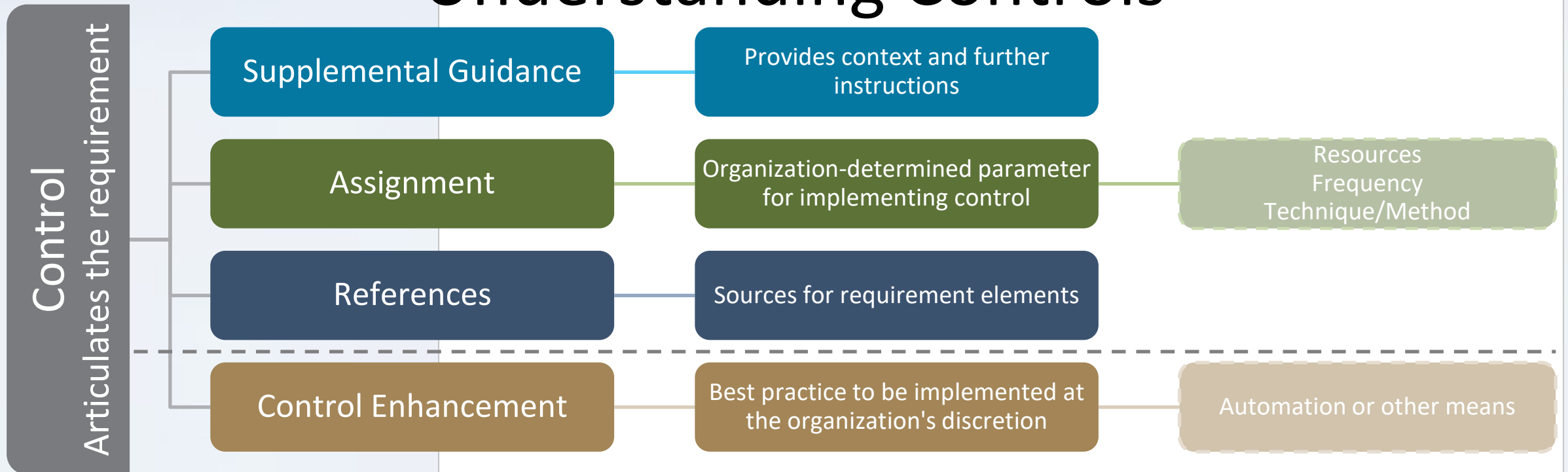
CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	IMPLEMENTED BY	ASSURANCE
PT-1	Policy and Procedures	O	✓
PT-2	Authority to Process Personally Identifiable Information	O	✓
PT-2(1)	DATA TAGGING	S	✓
PT-2(2)	AUTOMATION	O	✓
PT-3	Personally Identifiable Information Processing Purposes	O	
PT-3(1)	DATA TAGGING	S	✓
PT-3(2)	AUTOMATION	O	✓
PT-4	Consent	O	
PT-4(1)	TAILORED CONSENT	O	
PT-4(2)	JUST-IN-TIME CONSENT	O	
PT-4(3)	REVOCATION	O	
PT-5	Privacy Notice	O	
PT-5(1)	JUST-IN-TIME NOTICE	O	
PT-5(2)	PRIVACY ACT STATEMENTS	O	
PT-6	System of Records Notice	O	
PT-6(1)	ROUTINE USES	O	
PT-6(2)	EXEMPTION RULES	O	
PT-7	Specific Categories of Personally Identifiable Information	O	
PT-7(1)	SOCIAL SECURITY NUMBERS	O	
PT-7(2)	FIRST AMENDMENT INFORMATION	O	
PT-8	Computer Matching Requirements	O	

Appendix J - 88-53r5 Crosswalk

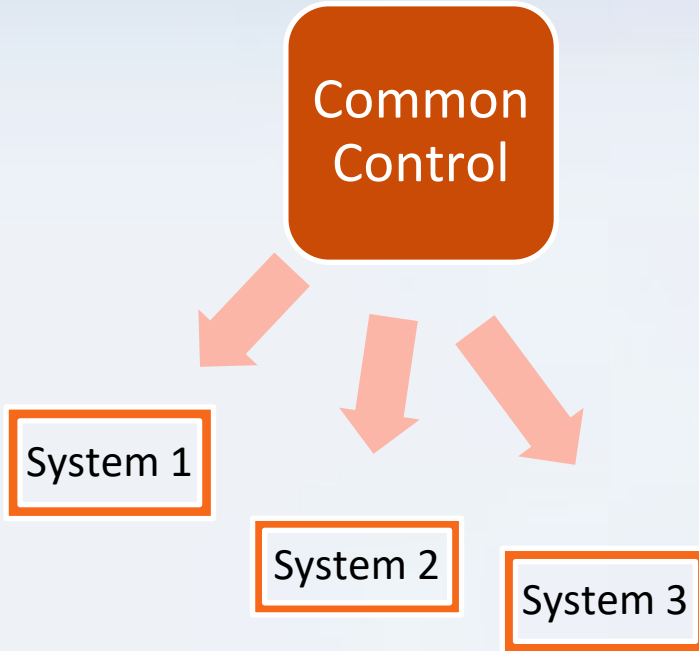
Get updates from [NIST](#)

800-53 Rev. 4 (Appendix J) Control	800-53 Rev. 5 Controls
AP-1: Authority to Collect	PT-2: Authority to Process Personally Identifiable Information
AP-2: Purpose Specification	PT-3: Personally Identifiable Information Processing Purposes
AR-1: Governance and Privacy Program	PIV-3: Information Security and Privacy Resources PIV-18: Privacy Program Plan PIV-19: Privacy Program Leadership Role PIV-23: Data Governance Body
AR-2: Privacy Impact and Risk Assessment	RA-3: Risk Assessment RA-8: Privacy Impact Assessment
AR-3: Privacy Requirements for Contractors and Service Providers	SA-4: Acquisition Process SA-9: External System Services
AR-4: Privacy Monitoring and Auditing	CA-7: Continuous Monitoring
AR-5: Privacy Awareness and Training	AT-2: Awareness Training AT-3: Role-based Training PL-4: Rules of Behavior
AR-6: Privacy Reporting	PIV-27: Privacy Reporting
AR-7: Privacy-Enhanced System Design and Development	PL-8: Security and Privacy Architectures PL-43: Enterprise Architectures PT-2: Authority to Process Personally Identifiable Information PT-2(1): Authority to Process Personally Identifiable Information Data Tagging PT-2(2): Authority to Process Personally Identifiable Information Automation PT-3: Personally Identifiable Information Processing Purposes PT-3(1): Personally Identifiable Information Processing Purposes Data Tagging PT-3(2): Personally Identifiable Information Processing Purposes Automation SI-18: Personally Identifiable Information Quality Operations SI-18(1): Personally Identifiable Information Quality Operations Automation Support SI-18(2): Personally Identifiable Information Quality Operations Data Tags

Understanding Controls



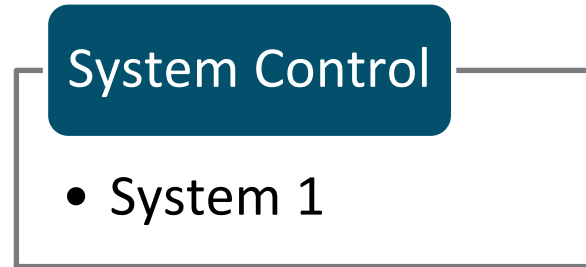
Control Types



Common Controls

Single implementation leveraged and used uniformly across the organization

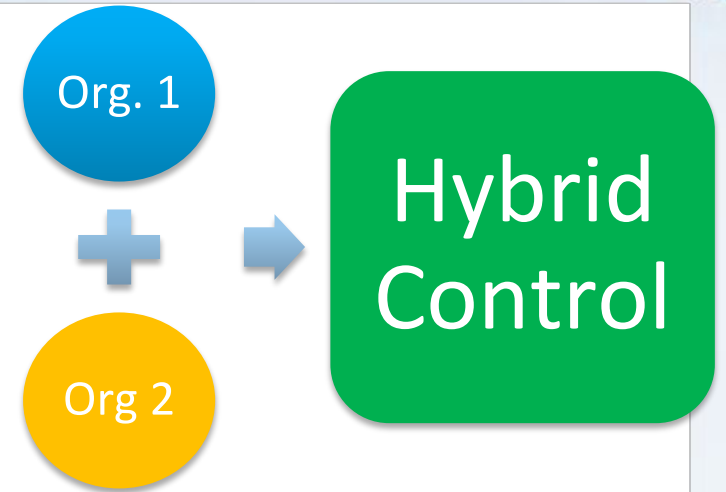
- PT-1 Policy and Procedures



System Controls

Implementation is unique to the specific system

- May leverage a standard approach
- PT-2 Authority to Process PII



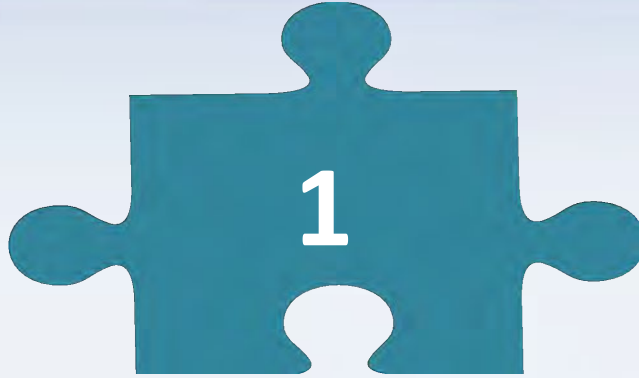
Hybrid Controls

Implementation is split between two or more elements of an organization

- PT3(1) PII Processing Purposes: Data Tagging

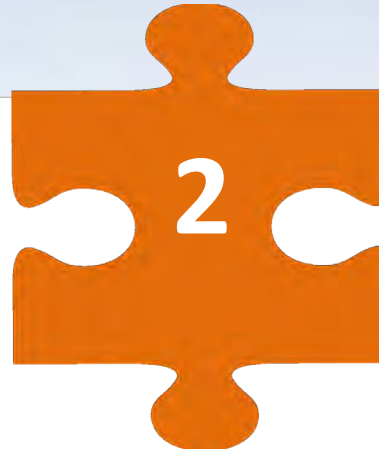
Capturing the implementation approach in the Privacy Plan promotes uniform understanding and execution and increases compliance.

Implementation Planning by SAOP



Establish Organization Approach

1. Determine common controls
2. Set assignment parameters where applicable
3. Document and Approve Plan
4. Disseminate and Educate
5. Implement common controls



System/Program Implementation

1. Select and implement privacy controls based on organization's privacy requirements and the need to protect PII
 - Document in PTA
2. Coordinate privacy control selection and implementation with business owners, CISO, CIO
 - Document in PIA and SORN



Assess Compliance

1. Develop Assessment Plan (use NIST SP 800-53A)
2. Conduct Assessment
 1. Are controls implemented?
 2. Do the controls reduce risk as intended?
3. Remediate

Privacy Plan

- May be at the organizational or system specific level.
- Organizations have flexibility in how they choose to document a
- Examples include a strategic framework document, PTA, or PIA.
- May be stand-alone or integrated with a security plan



Privacy Supported by Security

EXERCISE



Department of Space Travel and Albedo Research

Terrestrial Rendezvous and Explorer Knowledge

Mission to Mars (M2M)

You'll need: NIST SP 800-53 rev 5, available [here](#):

Go to p. 451



Mission to Mars

Scenario

- Department directed to establish a program to select member of the public for Mission to Mars
- Previous efforts failed in part because privacy concerns were not addressed in the design/build phase
- System must undergo full privacy and security risk assessment before any data about members of the public is used

System/Business Process Description

- Public Website
- Mobile Application
- Databases
 - Storage
 - Access/Data sharing
- Business Intelligence Analytical Engine
- Workflow processing
- Reporting tool
- C-High, I-Moderate, A-Low

STAR TREK M2M 001 - SORN

- Purpose:
 - Collect and maintain records related to the qualification, evaluation, training, certification, and selection of space cadets
- Location
 - Contractor: Klingon Enterprises, Lieutenant Commander Worf, First City, Q'onoS
 - COR: Lieutenant Commander Data, Omicron Thet
- System Manager
 - Captain James T. Kirk, Starship Enterprise
- Authority
 - Federation Exploration Order 001 - Where No Person Has Gone Before
- Categories of Individuals
 - Applicants for Mars exploration mission
- Disposal
 - Unsuccessful applicants
 - 18 months after selection cycle, records needed in the event that successful applicants do not complete process
 - Successful applicants
 - 5 years after return from Mars

STAR TREK M2M 001 - SORN cont.

- Categories of Records

- Applications

- Contact Information (name, address [physical and electronic], phone)
 - Social Media account names
 - Biographic Information (date of birth, birth location, gender, height, weight)
 - Transcripts (institutions, courses, grades)
 - Recommendations
 - Essays
 - Species

- Identity Verification

- Contact Information
 - Biometrics (fingerprint, retinal scan)
 - Species
 - Citizenship
 - Federation #

- Medical Clearance and Certification

- Physical and mental health records
 - Results of medical exams administered by STAR TREK
 - Biological samples and outcomes

- Evaluation Board outcomes

- Training Records

- Record Sources

- Applicants

- References Identified by Applicants

- Schools

- Medical Officers

- Federation Officials

- Routine Uses

- Institutions and Organizations included on resumes for the purposes of verifying information provided

- SecOps for purposes of determining if individual poses threat to the Federation

- Starfleet Academy for purposes of determining qualifications and fitness for space travel

- Contractors for purposes of administering systems

- Klingon High Council to provide combat training

- Ferengi Acquisition Association to determine if individuals have engaged in fraud

Group Exercise - Operationalizing the FIPPs

Questions to Think About

- What technical capabilities would help enforce “policy” established in SORN?
- What “evidence” would you want to examine?
- How would you gather evidence?
- How would you analyze the evidence?

FIPPs

- Authority and Purpose
- Accountability, Audit, Risk Management
- Data Quality and Integrity
- Data Minimization and Retention
- Individual Participation and Redress
- Security
- Transparency
- Use Limitation

PT-2 Authority to Process PII

Control Identifier	Control/Control Enhancement Name	Control Text	Discussion	Related Controls
PT-2	Authority to Process Personally Identifiable Information	<p>a. Determine and document the [Assignment: organization-defined authority] that permits the [Assignment: organization-defined processing] of personally identifiable information; and</p> <p>b. Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is authorized.</p>	<p>The processing of personally identifiable information is an operation or set of operations that the information system or organization performs with respect to personally identifiable information across the information life cycle. Processing includes but is not limited to creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal. Processing operations also include logging, generation, and transformation, as well as analysis techniques, such as data mining.</p> <p>Organizations may be subject to laws, executive orders, directives, regulations, or policies that establish the organization's authority and thereby limit certain types of processing of personally identifiable information or establish other requirements related to the processing. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such authority, particularly if the organization is subject to multiple jurisdictions or sources of authority. For organizations whose processing is not determined according to legal authorities, the organization's policies and determinations govern how they process personally identifiable information. While processing of personally identifiable information may be legally permissible, privacy risks may still arise. Privacy risk assessments can identify the privacy risks associated with the authorized processing of personally identifiable information and support solutions to manage such risks.</p> <p>Organizations consider applicable requirements and organizational policies to determine how to document this authority. For federal agencies, the authority to process personally identifiable information is documented in privacy policies and notices, system of records notices, privacy impact assessments, PRIVACT statements, computer matching agreements and notices, contracts, information sharing agreements, memoranda of understanding, and other documentation.</p> <p>Organizations take steps to ensure that personally identifiable information is only processed for authorized purposes, including training organizational personnel on the authorized processing of personally identifiable information and monitoring and auditing organizational use of personally identifiable information.</p>	AC-2, AC-3, CM-13, IR-9, PM-9, PM-24, PT-1, PT-3, PT-5, PT-6, RA-3, RA-8, SI-12, SI-18.
PT-2(1)	Authority to Process Personally Identifiable Information Data Tagging	Attach data tags containing [Assignment: organization-defined authorized processing] to [Assignment: organization-defined elements of personally identifiable information].	Data tags support the tracking and enforcement of authorized processing by conveying the types of processing that are authorized along with the relevant elements of personally identifiable information throughout the system. Data tags may also support the use of automated tools.	AC-16, CA-6, CM-12, PM-5, PM-22, PT-4, SC-16, SC-43, SI-10, SI-15, SI-19.
PT-2(2)	Authority to Process Personally Identifiable Information Automation	Manage enforcement of the authorized processing of personally identifiable information using [Assignment: organization-defined automated mechanisms].	Automated mechanisms augment verification that only authorized processing is occurring.	CA-6, CM-12, PM-5, PM-22, PT-4, SC-16, SC-43, SI-10, SI-15, SI-19.

AC-21 Information Sharing

Control Identifier	Control/Control Enhancement) Name	Control Text	Discussion	Related Controls
AC-21	Information Sharing	<p>a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and</p> <p>b. Employ [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing and collaboration decisions.</p>	Information sharing applies to information that may be restricted in some manner based on some formal or administrative determination. Examples of such information include, contract-sensitive information, classified information related to special access programs or compartments, privileged information, proprietary information, and personally identifiable information. Security and privacy risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to these determinations. Depending on the circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program or compartment. Access restrictions may include non-disclosure agreements (NDA). Information flow techniques and security attributes may be used to provide automated assistance to users making sharing and collaboration decisions.	AC-3, AC-4, AC-16, PT-2, PT-7, RA-3, SC-15.
AC-21(1)	Information Sharing Automated Decision Support	Employ [Assignment: organization-defined automated mechanisms] to enforce information-sharing decisions by authorized users based on access authorizations of sharing partners and access restrictions on information to be shared.	Automated mechanisms are used to enforce information sharing decisions.	None.
AC-21(2)	Information Sharing Information Search and Retrieval	Implement information search and retrieval services that enforce [Assignment: organization-defined information sharing restrictions].	Information search and retrieval services identify information system resources relevant to an information need.	None.

PT-4 Consent

Control Identifier	Control/Control Enhancement) Name	Control Text	Discussion	Related Controls
PT-4	Consent	Implement [Assignment: organization-defined tools or mechanisms] for individuals to consent to the processing of their personally identifiable information prior to its collection that facilitate individuals' informed decision-making.	Consent allows individuals to participate in making decisions about the processing of their information and transfers some of the risk that arises from the processing of personally identifiable information from the organization to an individual. Consent may be required by applicable laws, executive orders, directives, regulations, policies, standards, or guidelines. Otherwise, when selecting consent as a control, organizations consider whether individuals can be reasonably expected to understand and accept the privacy risks that arise from their authorization. Organizations consider whether other controls may more effectively mitigate privacy risk either alone or in conjunction with consent. Organizations also consider any demographic or contextual factors that may influence the understanding or behavior of individuals with respect to the processing carried out by the system or organization. When soliciting consent from individuals, organizations consider the appropriate mechanism for obtaining consent, including the type of consent (e.g., opt-in, opt-out), how to properly authenticate and identity proof individuals and how to obtain consent through electronic means. In addition, organizations consider providing a mechanism for individuals to revoke consent once it has been provided, as appropriate. Finally, organizations consider usability factors to help individuals understand the risks being accepted when providing consent, including the use of plain language and avoiding technical jargon.	AC-16, PT-2, PT-5.
PT-4(1)	Consent Tailored Consent	Provide [Assignment: organization-defined mechanisms] to allow individuals to tailor processing permissions to selected elements of personally identifiable information.	While some processing may be necessary for the basic functionality of the product or service, other processing may not. In these circumstances, organizations allow individuals to select how specific personally identifiable information elements may be processed. More tailored consent may help reduce privacy risk, increase individual satisfaction, and avoid adverse behaviors, such as abandonment of the product or service.	PT-2.
PT-4(2)	Consent Just-in-time Consent	Present [Assignment: organization-defined consent mechanisms] to individuals at [Assignment: organization-defined frequency] and in conjunction with [Assignment: organization-defined personally identifiable information processing].	Just-in-time consent enables individuals to participate in how their personally identifiable information is being processed at the time or in conjunction with specific types of data processing when such participation may be most useful to the individual. Individual assumptions about how personally identifiable information is being processed might not be accurate or reliable if time has passed since the individual last gave consent or the type of processing creates significant privacy risk. Organizations use discretion to determine when to use just-in-time consent and may use supporting information on demographics, focus groups, or surveys to learn more about individuals' privacy interests and concerns.	PT-2.
PT-4(3)	Consent Revocation	Implement [Assignment: organization-defined tools or mechanisms] for individuals to revoke consent to the processing of their personally identifiable information.	Revocation of consent enables individuals to exercise control over their initial consent decision when circumstances change. Organizations consider usability factors in enabling easy-to-use revocation capabilities.	PT-2.

SI-12 Information Management and Retention

Control Identifier	Control/Control Enhancement Name	Control Text	Discussion	Related Controls
SI-12	Information Management and Retention	Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.	Information management and retention requirements cover the full life cycle of information, in some cases extending beyond system disposal. Information to be retained may also include policies, procedures, plans, reports, data output from control implementation, and other types of administrative information. The National Archives and Records Administration (NARA) provides federal policy and guidance on records retention and schedules. If organizations have a records management office, consider coordinating with records management personnel. Records produced from the output of implemented controls that may require management and retention include, but are not limited to: All XX-1, AC-6(9), AT-4, AU-12, CA-2, CA-3, CA-5, CA-6, CA-7, CA-8, CA-9, CM-2, CM-3, CM-4, CM-6, CM-8, CM-9, CM-12, CM-13, CP-2, IR-6, IR-8, MA-2, MA-4, PE-2, PE-8, PE-16, PE-17, PL-2, PL-4, PL-7, PL-8, PM-5, PM-8, PM-9, PM-18, PM-21, PM-27, PM-28, PM-30, PM-31, PS-2, PS-6, PS-7, PT-2, PT-3, PT-7, RA-2, RA-3, RA-5, RA-8, SA-4, SA-5, SA-8, SA-10, SI-4, SR-2, SR-4, SR-8.	AC-16, AU-5, AU-11, CA-2, CA-3, CA-5, CA-6, CA-7, CA-9, CM-5, CM-9, CP-2, IR-8, MP-2, MP-3, MP-4, MP-6, PL-2, PL-4, PM-4, PM-8, PM-9, PS-2, PS-6, PT-2, PT-3, RA-2, RA-3, SA-5, SA-8, SR-2.
SI-12(1)	Information Management and Retention Limit Personally Identifiable Information Elements	Limit personally identifiable information being processed in the information life cycle to the following elements of personally identifiable information: [Assignment: organization-defined elements of personally identifiable information].	Limiting the use of personally identifiable information throughout the information life cycle when the information is not needed for operational purposes helps to reduce the level of privacy risk created by a system. The information life cycle includes information creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition. Risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to determining which elements of personally identifiable information may create risk.	PM-25.
SI-12(2)	Information Management and Retention Minimize Personally Identifiable Information in Testing, Training, and Research	Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: [Assignment: organization-defined techniques].	Organizations can minimize the risk to an individual's privacy by employing techniques such as de-identification or synthetic data. Limiting the use of personally identifiable information throughout the information life cycle when the information is not needed for research, testing, or training helps reduce the level of privacy risk created by a system. Risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to determining the techniques to use and when to use them.	PM-22, PM-25, SI-19.
SI-12(3)	Information Management and Retention Information Disposal	Use the following techniques to dispose of, destroy, or erase information following the retention period: [Assignment: organization-defined techniques].	Organizations can minimize both security and privacy risks by disposing of information when it is no longer needed. The disposal or destruction of information applies to originals as well as copies and archived records, including system logs that may contain personally identifiable information.	None.

How Can We Help?

QUESTIONS AND ANSWERS



Questions? We Have Answers

- **Who has the primary lead in implementing and assessing Privacy Controls?**
 - SAOP/CPO explicitly has primary responsibility
 - May choose to conduct control selection and implement on own or coordinate control selection with other stakeholders
 - Acknowledges privacy as a distinct discipline with a unique set of requirements that go beyond security
- **Who is responsible for implementing and assessing joint Privacy/Security Controls?**



More Questions – More Answers

- **Do all of the controls have to be implemented for every system?**
 - No. Apply controls in light of mission, business/operational needs, legal authorities (including specific exceptions and exceptions), and agency policy.
- **Can privacy controls be treated as common controls?**
 - Yes, consistent with the agency's particular mission needs. The determination of which controls to treat as common controls must be made by the SAOP, either alone or together with other agency stakeholders involved in risk management.



Claire W. Barrett

Deputy Chief Information Officer

Chief Privacy Officer

National Institute of Standards and Technology (NIST)

claire.barrett@nist.gov

240.532.0683



(b) (6)

Director, Mission Oversight and Compliance

Senior Component Official for Privacy

National Geospatial-Intelligence Agency

(b) (6)

(571) 557-0777





Federal Privacy Council

BACKUP SLIDES



Authorities and Policy Overview

- Federal Information Security Management Act of 2002
- OMB A-130
- NIST FIPS – Federal Information Processing Standards
 - Mandatory policies, including:
 - FIPS 199 – Security Categorization of Federal Information and Information Systems
 - FIPS 200 – Minimum Security Controls for Federal Information Systems
- NIST SP – Special Publications
 - Guidelines for use by departments and agencies, including:
 - Preparation of Security Plans (SP 800-18)
 - Applying the Risk Management Framework (SP 800-37)
 - Security and Privacy Controls for Federal Information Systems and Organizations (SP 800-53 rev 5)

FISMA Overview

- Federal Information Security Management Act of 2002
- Title III of E-Government Act of 2002
- Administered by:
Office of Management and Budget (OMB)
- Applies to: Executive Branch
 - Department of Defense (DoD) components
 - Intelligence Community (IC) agencies
 - Federal “civilian” departments and agencies

FISMA: Key Provisions

- Departments and agencies shall implement:
 - Security policies and procedures
 - Security awareness training
 - Periodic risk assessments
 - Testing and evaluation of security controls at least annually
 - Process to address security deficiencies
 - Incident response procedures
 - Continuity of operations plans and procedures

Additional FISMA Provisions

- Agencies required to conduct annual reviews and report to OMB
- OMB reports to Congress
- National Institute of Standards and Technology (NIST) is directed to develop security guidelines
- Updated with the Federal Information Security Modernization Act of 2014.

NIST Publications

FIPS – Federal Information Processing Standards

- Mandatory policies, including:
- FIPS 199 – Security Categorization of Federal Information and Information Systems
- FIPS 200 – Minimum Security Controls for Federal Information Systems

SP – Special Publications

- Guidelines for use by departments and agencies, including:
- Preparation of Security Plans (SP 800-18)
- Applying the Risk Management Framework (SP 800-37)
- Security and Privacy Controls for Federal Information Systems and Organizations (SP 800-53 rev 5)

OMB A-130 Appendix I

- Responsibilities for Protecting and Managing Federal Information Resources (<https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf>)
- Establishes minimum requirements for Federal information security programs and assigns responsibilities for the security of information and information systems.
 - Perform ongoing reauthorization of systems (replacing the triennial reauthorization process) to better protect agency information systems;
 - Continuously monitor, log, and audit user activity to protect against insider threats;
 - Periodically test response procedures and document lessons learned to improve incident response;
 - Encrypt moderate and high impact information at rest and in transit;
 - Ensure terms in contracts are sufficient to protect Federal information;
 - Implement measures to protect against supply chain threats;
 - Provide identity assurance for secure government services; and,
 - Ensure agency personnel are accountable for following security and privacy policies and procedures.

OMB A-130 Appendix I (cont)

- Information Security Requirements
 - a) Ensure that the CIO designates a senior agency information security officer to develop and maintain an agency-wide information security program in accordance with the Federal Information Security Modernization Act of 2014 (FISMA);
 - b) Protect information in a manner commensurate with the risk that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information; and
 - c) Implement security policies issued by OMB, as well as requirements issued by the Department of Commerce, the Department of Homeland Security (DHS), the General Services Administration (GSA), and the Office of Personnel Management (OPM). This includes applying the standards and guidelines contained in the NIST FIPS, NIST SPs (e.g., 800 series guidelines), and where appropriate and directed by OMB, NIST Interagency or Internal Reports (NISTIRs).

Rev 4 App J / Rev 5 Comparison

800-53 Rev 4 (Appendix J) Control	800-53 Rev. 5 Controls
AP-1: Authority to Collect	PT-2: Authority to Process Personally Identifiable Information
AP-2: Purpose Specification	PT-3: Personally Identifiable Information Processing Purposes
AR-1: Governance and Privacy Program	PM-3: Information Security and Privacy Resources PM-18: Privacy Program Plan PM-19: Privacy Program Leadership Role PM-23: Data Governance Body
AR-2: Privacy Impact and Risk Assessment	RA-3: Risk Assessment RA-8: Privacy Impact Assessment
AR-3: Privacy Requirements for Contractors and Service Providers	SA-4: Acquisition Process SA-9: External System Services
AR-4: Privacy Monitoring and Auditing	CA-7: Continuous Monitoring
AR-5: Privacy Awareness and Training	AT-2: Awareness Training AT-3: Role-based Training PL-4: Rules of Behavior

Rev 4 App J / Rev 5 Comparison

AR-6: Privacy Reporting	PM-27: Privacy Reporting
AR-7: Privacy-Enhanced System Design and Development	PL-8: Security and Privacy Architectures PM-7: Enterprise Architectures PT-2: Authority to Process Personally Identifiable Information PT-2(1): Authority to Process Personally Identifiable Information Data Tagging PT-2(2): Authority to Process Personally Identifiable Information Automation PT-3: Personally Identifiable Information Processing Purposes PT-3(1): Personally Identifiable Information Processing Purposes Data Tagging PT-3(2) Personally Identifiable Information Processing Purposes Automation SI-18: Personally Identifiable Information Quality Operations SI-18(1): Personally Identifiable Information Quality Operations Automation Support SI-18(2): Personally Identifiable Information Quality Operations Data Tags

Rev 4 App J / Rev 5 Comparison

AR-8: Accounting of Disclosures	PM-21: Accounting of Disclosures
DI-1: Data Quality	PM-22: Personally Identifiable Information Quality Management SI-18: Personally Identifiable Information Quality Operations
DI-2: Data Integrity and Data Integrity Board	PM-24: Data Integrity Board SI-7: Software, Firmware, and Information Integrity
DM-1: Minimization of Personally Identifiable Information	SA-8(33): Security and Privacy Engineering Principles Minimization PM-5(1): System Inventory Inventory of Personally Identifiable Information SI-12(1): Information Management and Retention Limit Personally Identifiable Information Elements
DM-2: Data Retention and Disposal	MP-6: Media Sanitization SI-12: Information Management and Retention SI-12(3): Information Management and Retention Information Disposal

Rev 4 App J / Rev 5 Comparison

DM-3: Minimization of PII used in Testing, Training, and Research	PM-25: Minimization of PII used in Testing, Training, and Research SI-12(2): Information Management and Retention Minimize Personally Identifiable Information in Testing, Training and Research
IP-1: Consent	PT-4: Consent
IP-2: Individual Access	AC-3(14): Access Enforcement Individual Access PM-22: Personally Identifiable Information Quality Management
IP-3: Redress	IR-7: Incident Response Assistance PM-22: Personally Identifiable Information Quality Management SI-18: Personally Identifiable Information Quality Operations SI-18(4): Personally Identifiable Information Quality Operations Individual Requests SI-18(5): Personally Identifiable Information Quality Operations Notice of Correction or Deletion

Rev 4 App J / Rev 5 Comparison

IP-4: Complaint Management	PM-26: Complaint Management
SE-1: Inventory of Personally Identifiable Information	PM-5(1): Sytem Inventory Inventory of Personally Identifiable Information
SE-2: Privacy Incident Response	IR-8: Incident Response Plan IR-8(1): Incident Response Plan Breaches
TR-1: Privacy Notice	PT-5: Privacy Notice PT-5(1): Privacy Notice Just-In-Time Notice
TR-2: System of Records Notices and Privacy Act Statements	PT-5(2): Privacy Notice Privacy Act Statements PT-6: System of Records Notice
TR-3: Dissemination of Privacy Program Information	PM-20: Dissemination of Privacy Program Information
UL-1: Internal Use	PT-3: Personally Identifiable Information Processing Purposes
UL-2: Information Sharing with Third Parties	AC-21: Information Sharing PT-2: Authority to Process Personally Identifiable Information PT-3: Personally Identifiable Information Processing Purposes

FPC Boot Camp: Approaches to Emerging Tech and Agile methods



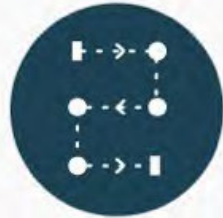
Federal Privacy Council

Goals and Outcomes

- Privacy approaches to Modernization/Digital First environments
- Agile Methodology, DevOps and Privacy Engineering
- Ensure your voices are heard early and often throughout the information lifecycle
- How might you work in a more Agile way?
- Where can you go for technical training and resources?

DevOps vs. Agile

DevOps



Periodic delivery



Large teams



Self-reliance



Immediate implementation



Collaboration



Broad skill set required

Agile



Continuous delivery



Small teams



Customer feedback



Planning before implementation



Communication



Narrow skill set required

Assessing Privacy Risks of New Technologies - Robotics Process Automation (RPA)

- Background
- The Problem
- What is Robotics Process Automation (RPA)?
- A Solution
- A Case Study
- Role Playing Exercise

Background

Presidents Management Agenda – IT Modernization

Goal

Modernize IT to Increase Productivity
and Security.

Opportunity

There are opportunities to: expand the use of modern commercial technologies that are effective, economical, and secure; reduce the impact of cybersecurity risks by safeguarding IT systems, sensitive data, and networks; leverage common solutions and innovative practices to improve efficiency, increase security, and ultimately meet citizens' needs.

The Problem

- How can we free up employees to spend more time on higher impact activities to increase productivity and increase engagement?
 - Employee productivity has plateaued, while the workload for mission critical activities increases.
 - Employees spend a lot of time doing data entry. To increase the quality of life of employees & increase productivity, their time could be better spent doing data analysis.

Potential Solution

- Robotics Process Automation (RPA) is automation of a manual process that is largely rules based, structured, and repetitive using software robots, also called bots.
- A RPA tool maps a process for a robot to follow so that the bot can operate in place of a human.
- RPA technology generally does not require programming experience, although experience with scripting and macros is helpful.
- RPA technology offers “bot management” consoles.

Attended vs. Unattended Bots

Attended Bots

- Reside on a local workstation
- Triggered by humans
- Ideal for processes that require human interaction

Unattended Bots

- Can be deployed to physical or virtual environments
- Operate without human touch
- Can run in batch mode
- Can be accessed remotely

Benefits & Risks

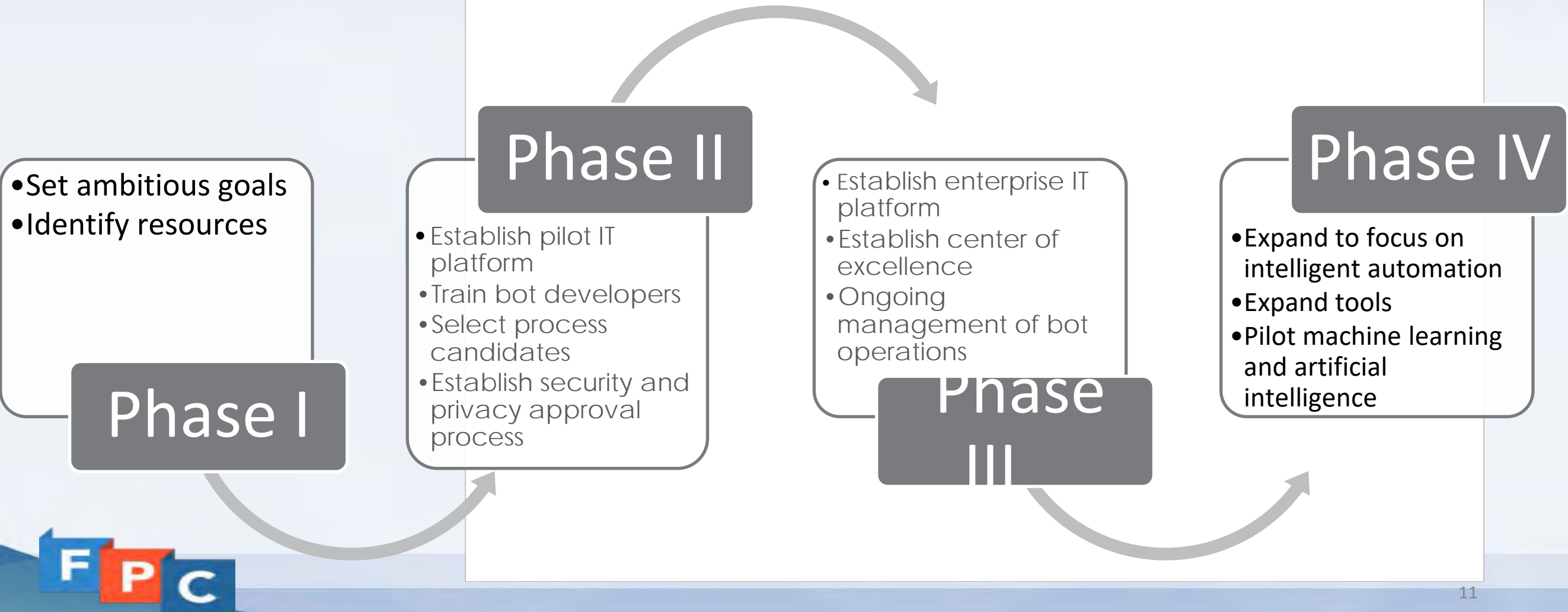
Benefits

- Reduce cycle times
- Better customer experience
- Lower operating costs
- Minimal error rates
- Better management capabilities
- Transactional to analytical culture

Risks

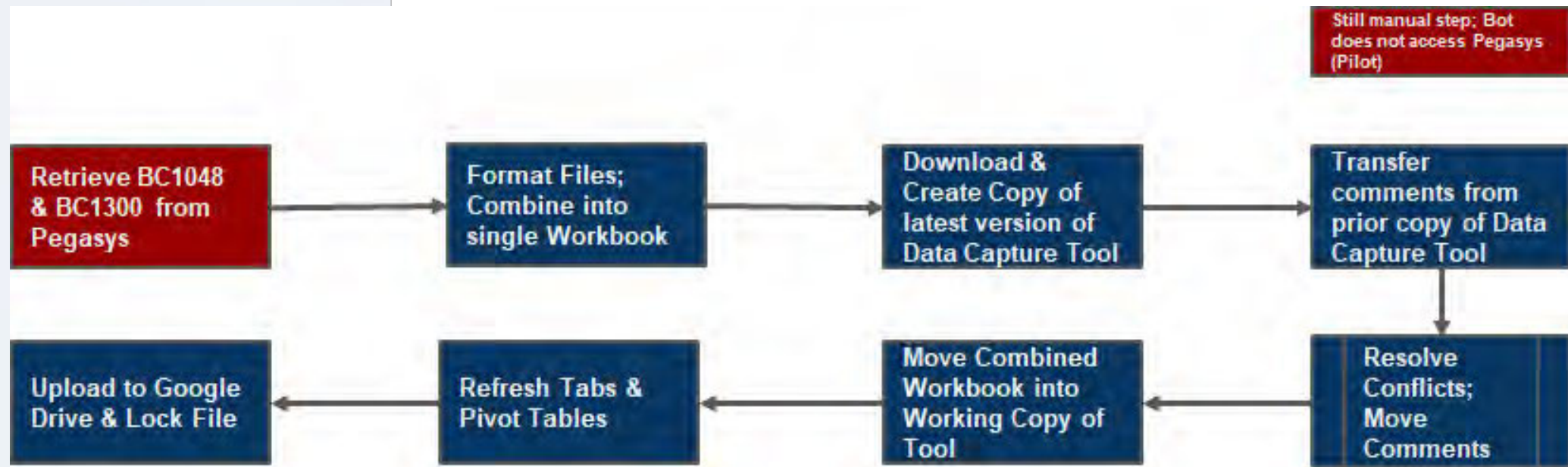
- Dependency on systems to be accurate, reliable, and stable
- Reliant on business units analyzing and prioritizing processes upfront
- If problematic data actions (incidents) occur, they may scale more quickly

RPA Program Approach



RPA Case Study –

Goal: Use a bot to process uncollected balances



RPA Case Study: Manual vs. Bot

Result: A federal agency reduced manual labor by 98.3%

Manual

- 6,000 min/month (100 hours/month)
- Run once a week (too time consuming to run more often manually)
- All manual process

Bot

- 5 min per day for bot steward (100 min/month)
- Run daily
- Data refreshed daily, which speeds up workflow

Role Playing Exercise



Key Takeaways & Privacy Equities

1. **RPA programs across the federal government are growing.** In FY21, federal RPA programs significantly grew and matured.
 - a. A subset of these programs handle PII
2. **More automations give federal employees more time.** The federal RPA community has reduced over 1.4M hours (and counting) of low-value work across the government to date. RPA helps federal employees do more important work.
 - a. Breach mitigation may take new forms
3. **Federal agencies want RPA programs.** 65% of RPA programs have over 20 automations in their pipelines; 75% of emerging RPA programs plan to launch a pilot within the next 12 months.
 - a. Strategic planning of resources will help Privacy offices prioritize
4. **RPA programs are using Intelligent Automation (IA) solutions.** 32% of RPA programs have incorporated IA features: like machine learning, artificial intelligence, image recognition, chat bots, and natural language processing.
 - a. A growth mindset (a.k.a. lifetime learners) remains a highly sought after feature of Privacy professionals

Key Takeaways & Privacy Equities (continued)

5. **RPA programs enhanced their accountability and oversight.** 68% of federal RPA programs are currently centralized with program management. Several are becoming ready for audits and developing dashboards for reporting.
 - a. Privacy documentation can help
6. **RPA programs built productive relationships with IT departments.** Programs continue to work with IT departments to get approvals and ensure proper security controls.
 - a. Work with Privacy offices to ensure proper privacy controls
7. **RPA programs adopted more sophisticated technology platforms.** 60% of the programs use enterprise platforms. Most are using the cloud.
 - a. Reflect these changes in Privacy documentation (e.g., system of records notices)
8. **RPA programs developed varied team structures.** Program teams balance federal and contract employees.
 - a. Include Privacy clauses in relevant contracts

Resources

- FPC Committees and Working Groups
- NIST Privacy Engineering
- Digital.gov
- Centers of Excellence and Communities of Practice

Contact Information

Richard Speidel

- Chief Privacy Officer
- Richard.Speidel@gsa.gov

Marcela Souaya

- Senior Policy Analyst
- msouaya@cftc.gov



Federal Privacy Boot Camp

Spring 2022 Agenda

Session 7: Contracts & Web Policies

Title Session 7: Contracts & Web Policies

Date May 6, 2022 (Friday)

Location Virtual

Time 1:00 PM - 5:00 PM

Time	Topic	Presenter(s)
1:00 PM – 2:00 PM	Contracts	Alex Tang (FTC)
2:00 PM – 2:10 PM	Break	
2:10 PM – 3:00 PM	Cont'd	
3:00 PM – 4:00 PM	Web Policies	(b) (7)(C) (DHS)
4:00 PM – 4:10 PM	Break	
4:10 PM – 5:00 PM	Cont'd	

Required Reading

- OMB's Privacy Guidance: <https://www.fpc.gov/resources/omb/>

Suggested Reading

- [M-10-22](#) (Web Measurement and Customization)
- [M-10-23](#) (Third-Party Websites and Applications)
- [Model Privacy Impact Assessment](#) (Third-Party Websites and Apps.)
- [M-03-22](#) (Implementing the Privacy Provisions of E-Gov.)
- [M-99-18](#) (Privacy Policies)
- [M-05-04](#) (Use of Federal Agency Public Websites)
- [DHS: Mobile Application Playbook \(MAP\)](#)
- [CIO Council: Privacy Best Practices for Social Media](#)
- [CIO Council: Recommendations for Standardized Implementation of Digital Privacy Controls](#)
- [FTC: Online Tracking](#)

Attendance and Credit

Boot Camp staff will record attendance via the virtual platform during each session. This record will be used to determine your applicable credits at the conclusion of the training.

- The Federal Privacy Boot Camp qualifies as a training for CLP credit for federal employees. The entire camp is worth 32 credits, 4 per session over 8 sessions.
- If a session ends early, attendees that stay for the full session still earn 4 credits. Those with late arrival or early departure will have credit hours rounded up to the nearest hour.

Should you not be able to attend a session, please give Boot Camp staff advanced notice as soon as possible. If you miss more than two (2) sessions without notice, you will receive a notification that you will be dropped from the Boot Camp if you miss a third.

Session Materials

Weekly emails with slides and materials will be distributed to attendees. Materials will also be posted on the [Privacy Boot Camp MAX page](https://community.max.gov/x/ZwU1S) (<https://community.max.gov/x/ZwU1S>).

Listservs

The Privacy Boot Camp Listserv (privacy-bootcamp@listserv.gsa.gov) has been created to facilitate ongoing discussion during this program. This listserv is not actively moderated and instead will operate as an open forum for discussion. We encourage you to engage with one another through this platform to get to know your privacy peers across Government.

Please email the Privacy Council Inbox (privacy.council@gsa.gov) if you would like to be added as a subscriber to any of the following Privacy Council listservs:

- **PRIVACY-COUNCIL**: Broadest distribution to the Federal privacy community. Includes a bi-weekly Privacy Post newsletter. General announcements related to the FPC.
- **FPC-AIC and AIC-DISCUSSION**: List for the Agency Implementation Committee which hosts monthly calls that feature (1) updates from SAOP council meetings, (2) presentations, (3) guided discussions relating to privacy topics, and (4) open Q&A.
- **FPC-TI-AI**: List for the Artificial Intelligence Working Group within the FPC Technology and Innovation Working Group.
- **PRIVACY-JOBS**: Subscribers receive and are able to distribute federal privacy job announcements.

**Federal Privacy Boot Camp
Spring 2022**

PRIVACY AND CONTRACTS

**Alex Tang, Assistant General Counsel
National Science Foundation (NSF)**

Disclaimer: Views are my own, not necessarily those of NSF, the US Government, or any other individual or entity.



Federal Privacy Council



Contractor breach gave hackers keys to OPM data

Aaron Boyd, Senior Staff Writer

4:44 p.m. EDT June 25, 2015



(Photo: Mark Wilson/Getty Images)

f 132
CONNECT

TWEET

in 102
LINKEDIN

1
COMMENT

EMAIL

MORE

A breach of KeyPoint Government Solutions — a contractor used by federal agencies to conduct background checks — gave hackers the credentials needed to access sensitive employee data held by the Office of Personnel Management, the agency director confirmed Tuesday.

MORE STORIES



This Week in F Times: Private- come to State I
Nov. 26, 2015, 1:55



ANTHEM HEALTH CARE HACK SNARED FEDERAL EMPLOYEES WHO WEREN'T ANTHEM CUSTOMERS



Michael Cansoy/AP

f Share this
Tweet this
5
in Share 19
Print this article
Email this article
Increase size

A month after detecting a data breach, Anthem, a Blue Cross and Blue Shield federal employee benefit provider, either does not know or won't comment publicly on how many federal employee plan members are affected by the hack.

Over the past week, Anthem has disclosed more details on the extent of a December 2014 database compromise that allowed unidentified attackers to view sensitive personal information. The incident is now known to have affected current members of Anthem's own federal benefits BCBS plan, which includes 1.3 million



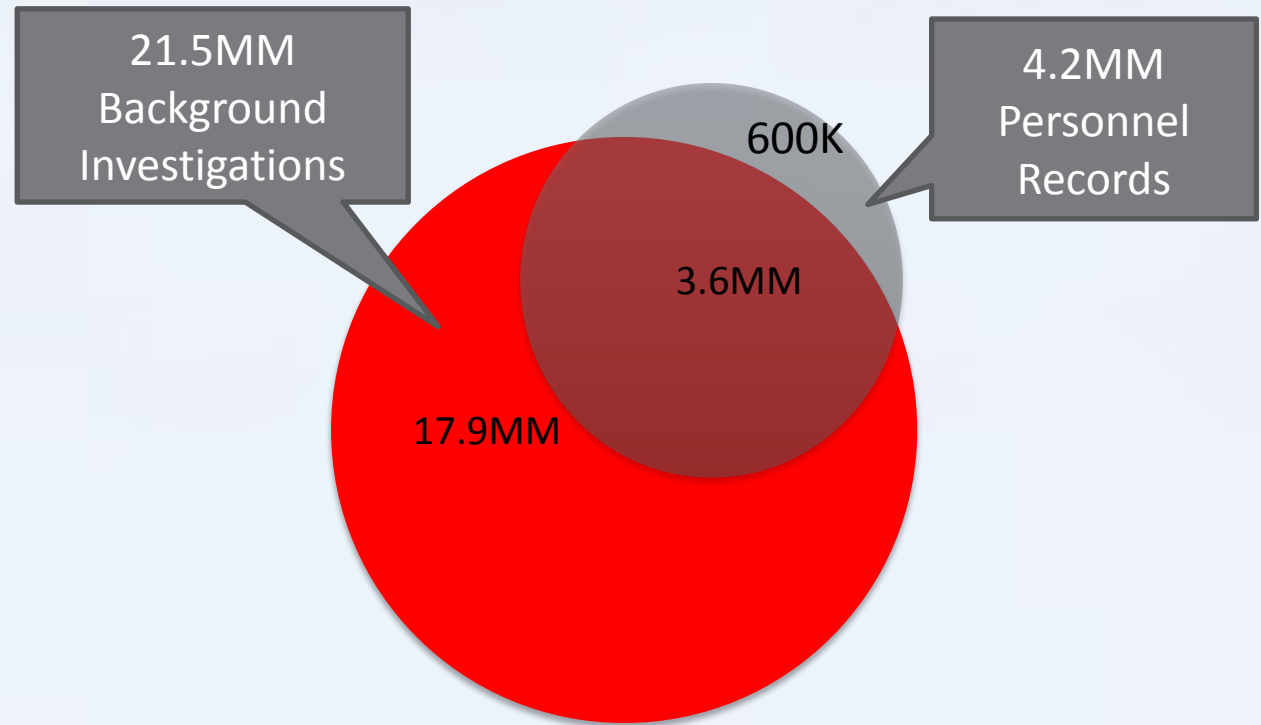
Federal Personnel Data Breaches

Two separate but related cyberincidents (2015)

- Approx. **21.5 million** background investigation records (e.g., SSN, fingerprints, passwords)
- Approx. **4.2 million** personnel records (e.g., full name, address, SSN)

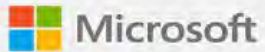
Total # Records Breached: **25.7 million**

Total # Affected Individuals: **22.1 million**



+

○



Supply Chain Security

- “Hackers targeted **SolarWinds** by deploying malicious code into its Orion IT monitoring and management software used by thousands of enterprises and government agencies worldwide”—[whatis.techtarget.com](https://www.techtarget.com/whatis/definition/solarwinds) (6/16/2021)
- “After an initial dormant period of up to two weeks, it retrieves and executes commands, called “Jobs,” that include the ability to **transfer files, execute files, profile the system, reboot the machine, and disable system services**. The malware masquerades its network traffic as the Orion Improvement Program (OIP) protocol and stores reconnaissance results within legitimate plugin configuration files **allowing it to blend in with legitimate SolarWinds activity**.”—[mandiant.com](https://www.mandiant.com/blog/solarwinds-incident) (12/13/2020)

Beyond breaches: other privacy risks of outsourcing?

- Unauthorized **collection, use, and sharing**
- Unauthorized **maintenance and retention**
- Greater potential loss of **data integrity, quality, and accuracy**
- Delegation of **privacy and security control** to others
- **Higher costs** to detect and remedy these issues

US Gov't Outsources Many PII Functions



Collection



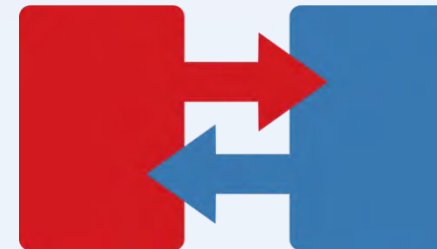
**Processing (e.g.,
merging) &
Analysis (e.g.,
reporting)**



Storage



Access & Retrieval



**Transfer &
Dissemination**



**Disposal &
Destruction**

How about your organization?

- **What goods or services do you outsource that could raise privacy or data security issues?**

Outline

I. Federal Contracting: Basic Rules, Concepts, and Terms

- Federal Acquisition Regulation (FAR)
- Contracting methods and contract types/vehicles
- Special issues presented by contracting, including enforcement/remedies

Outline

II. FAR Clauses Relating To Privacy and Data Security

- Privacy Act of 1974
- IT Privacy or Security Safeguards
- Basic Safeguarding of Covered Contractor Information Systems
- Privacy Training
- Rights in Data
- Kaspersky Labs
- Telecommunications and Video Surveillance Services or Equipment from China

Outline

II. FAR Clauses Relating To Privacy and Data Security

- Privacy Act of 1974
- IT Privacy or Security Safeguards
- Basic Safeguarding of Covered Contractor Information Systems
- Privacy Training
- Rights in Data
- Kaspersky Labs
- Telecommunications and Video Surveillance Services or Equipment from China

Outline

III. Other Privacy and Data Security Issues in Federal Contracts

- Incident Response
- Privacy Impact Assessments (PIAs)
- Non-Disclosure Agreements (NDAs)
- Records Management
- Web Services/Tracking
- Privacy Continuous Monitoring

IV. Final Group Exercise, Sources, Some Critical Lessons

I. FEDERAL CONTRACTING: BASIC RULES, CONCEPTS, AND TERMS

Federal Acquisition Regulation (FAR)

- A **uniform set of policies and procedures** for acquisitions by all Executive agencies.
- They are primarily intended to ensure **full and open competition**.
 - See generally Competition in Contracting Act (CICA), 41 U.S.C. 253
- They are also used to achieve **other public policy objectives**.
 - See, e.g., Clinger-Cohen Act (Federal Acquisitions Reform Act, IT Management Reform Act), Pub. L. 104-106, Divs. D & E)

Federal Acquisition Regulation (FAR)

- The FAR is issued under the authority of the **FAR Council (DOD, GSA, NASA)**
- Revisions are prepared and coordinated by the **Defense Acquisition Regulations Council (DAR Council)** and **Civilian Agency Acquisition Council (CAA Council)**
- The FAR and revisions are published and distributed by the **FAR Secretariat (GSA)**

Federal Acquisition Regulation (FAR)

- **Where can I find the FAR?**
 - 48 CFR §§ 1.000-52.303 (Parts 1 through 52)
 - Official text: www.ecfr.gov (Office of Federal Register)
 - Unofficial text: www.acquisition.gov (GSA/FAR Secretariat)
 - **FAR clauses** are contained in **FAR Part 52 (Subpart 52.2)**
- **What are FAR Supplements?**
 - **Defense FAR (DFAR)**, 48 CFR ch. 2 (§§ 201.104 et seq.)
 - **Homeland Security FAR (HSAR)**, 48 CFR ch. 30 (§§ 3000.101 et seq.)
 - **30+ other Federal agencies**

Federal Acquisition Regulation (FAR)

- Key Definitions (FAR 2.101)
 - **Contract** means “a **mutually binding legal relationship** obligating the seller to furnish the supplies or services . . . and the buyer to pay for them. It includes all types of commitments that **obligate the Government to an expenditure of . . . funds** . . . and that, except as otherwise authorized, are **in writing.**” FAR 2.101.

Federal Acquisition Regulation (FAR)

- Key Definitions (FAR 2.101)
 - ***Contracting officer*** means a person with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.
 - ***Contracting officer's representative (COR)*** means an individual, including a contracting officer's technical representative (COTR), designated and authorized in writing by the contracting officer to perform specific technical or administrative functions.

Basic Contracting Methods

Acquisition Method (FAR Part)	Key procedures, terminology, and forms
Simplified Acquisition Procedures (Part 13) for goods/services up to \$10K micro-purchase threshold (MPT); \$250K small acquisition threshold (SAT); and commercial items below \$7.5MM	Request For Quote/Quotation (RFQ) Purchase Order (PO)—Gov't offer to purchase (see GSA Form 300) Blanket Purchase Agreement (BPA) for repetitive needs Task Order (TO) placed against existing contract, BPA, or required sources Payment by purchase card, imprest fund, or certified invoice
Sealed Bidding (Part 14)	Fixed-price contracts Invitation for, submission, opening, and evaluation of bids Contract Award: Uniform Contract Format (see SF26) or Simplified Contract Format (see SF1447)
Contract By Negotiation (Part 15)	Fixed-price or cost contracts Solicitation/Request for Proposal (RFP) Technical evaluation and best-value determination Contract award: Uniform Contract Format, see SF26

Special Contracting Programs and Procedures

- **Required sources (FAR Part 8)**
 - Federal Prison Industries
 - Ability One (blind/disabled)
- **Other than full and open competition (FAR Subpart 6.3)**
 - Only one responsible source (“sole-source” contract)
 - Other exceptions (e.g., unusual and compelling urgency, expert litigation services, national security)
- Acquisition of **commercial items (FAR Part 12)**
- **Set-asides** for small business, 8(a), women-owned, etc. **(FAR Part 19)**

GSA Contracting Programs

- **Federal Supply Schedule (FSS) (FAR Subpart 8.4)**
 - Multiple Award Schedule (MAS) contracts awarded by GSA or VA
 - For similar or comparable supplies/services with more than one supplier
 - At varying prices (aka “task order contracts” or “delivery order contracts”)
- **GSA Government-Wide Acquisition Contracts (GWACs)**
 - Task/delivery order contracts for IT services and IT services-based solutions (e.g., 8(a) STARS II, Alliant, VETS (SDVOSB))
- **GSA Federal Risk and Authorization Mgt. Program (FedRAMP), www.fedramp.gov**
 - Provides a standardized approach to security authorizations for cloud service offerings
 - Customer agencies must still perform their own PIAs based on specific PII and uses
 - Cloud services can create overseas data storage and foreign surveillance issues (CONUS clause)

Privacy/Security Challenges in Contracting

- Your ability to include privacy or information security requirements may depend on the contracting method and vehicle
 - Uniform Contract Format (negotiated contracts): see **Section I (clauses incorporated by reference)**, see also **Section C (statement of work)** and **Section H (special requirements)**
 - **Simplified Contract Format:** FAR clauses may not be used unless “absolutely necessary”
 - **Purchase cards, imprest funds, certified invoices:** often no written or negotiated agreement (e.g., GSA Form 300 (purchase order))

Privacy/Security Challenges in Contracting

- **“Take it or leave it” problem: contract language may be pre-established, difficult to find or obtain, and non-negotiable**
 - Purchase cards, imprest funds, certified invoices
 - Federal Supply Schedule and other GSA-awarded contracts
 - Commercial off-the-shelf software (COTS)
 - IT Service Level Agreements (SLAs)
- **Privacy language for one contractor may not be appropriate for another (one size does not fit all)**

Privacy/Security Challenges in Contracting

- **Your organization's acquisitions program may have privacy and security "blind spots"**
 - Purchase cards, imprest funds, certified invoices
 - Emergency and other sole-source purchases
 - Inter-agency and multi-agency acquisitions
 - Federal grants and cooperative agreements (not covered by FAR)

Privacy/Security Challenges in Contracting

- Privacy oversight of contractors can be more difficult and costly
 - Lack of **visibility** into contractor operations (esp. if off-site)
 - Lack of direct **control** over their equipment and staff
 - Lack of legal **privity** with subcontractors
 - **Third-party audits and monitoring** are expensive, and who pays?

Privacy/Security Challenges in Contracting

Do contractors understand how the Federal Government defines PII?

See OMB 17-12:

“The term PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is **linked or linkable to a specific individual**. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. To determine whether information is PII, the agency shall perform an assessment of the **specific risk that an individual can be identified using the information with other information** that is linked or linkable to the individual. In performing this assessment, it is important to recognize that **information that is not PII can become PII whenever additional information becomes available--in any medium or from any source--that would make it possible to identify an individual.**”

Who am I?



Images: freefoodphotos.com CC 3.0, J. Morano CC 2.0, Melika CC 2.0

Contract Enforcement/ Remedies

Q: Can the Federal Government sue a contractor or subcontractor to enforce a privacy or data security requirement in its contract?

☐ Yes

☐ No

A: In some cases, yes, but such lawsuits are relatively uncommon, they are typically difficult, time-consuming, and costly to pursue, and the Government may not prevail. In short, suing is not normally an effective or available contract enforcement strategy.

Contract Enforcement/Remedies

Why?

- **Agencies are usually on the defensive rather than the offensive** (e.g., GAO bid protests, Contract Claims Act lawsuits)
- **Most agencies do not have their own contract litigating authority**
 - Agencies must convince the Justice Dep't (e.g., U.S. Attorney) to sue on their behalf
 - Usually requires a **violation of law**, not just violating contract terms and conditions (e.g., Privacy Act criminal penalties, False Claims Act)
 - **Fraud or substantial financial harm** must normally be alleged
- **Except in defense contracts, the Government rarely obtains a specific performance remedy, except by settlement** (i.e., requiring that the contractor do what it promised to do rather than pay damages or reimburse)

Quad/Graphics, Inc. Agrees to Pay \$750,000 to Settle Allegations Regarding Work for GPO

*Source: U.S. Attorney's Office, Dist. Of
Columbia (6/15/2016 Press Release)*

- The Sussex, WI, company had a **Gov't Printing Office (GPO) contract** to print **SSA forms** containing PII protected by Privacy Act of 1974
- A **GPO IG investigation** found security issues at the company's Chalfont, PA, plant
- It failed to **dispose of waste** in accordance with GPO procedures
- **Malfunctioning security cameras** were used to monitor production runs and bale room
- **Unauthorized employees** did not have required **background checks**
- **Sign-in sheets were altered** to conceal unauthorized employees who accessed secure work area
- **Settlement** included changes to **training program** for employees with access to PII, and **physical layout** of its printing facility to maximize security of PII
- **No admission of liability** and the **contract apparently was not terminated**

Contract Enforcement/Remedies

1. **Performance-based standards** for payment and withholding payment (non-acceptance) in service contracts
 - A **performance work statement (PWS)**;
 - **Measurable performance standards** (i.e., in terms of quality, timeliness, quantity, etc.) and the **method of assessing contractor performance** against performance standards; and
 - **Performance incentives** where appropriate, that correspond to the performance standards in the contract.
2. **Liquidated damages or indemnification clauses** (e.g., contractor liable for failure to perform, or for injury/damage caused to others, such as a data breach)
3. **Inspection and Acceptance—Quality Assurance, FAR Part 46** (e.g., max. error rate to ensure data quality, accuracy)
4. **Letter of concern, cure notice, show cause notice** (written notice of problems and an opportunity and deadline to fix them)
5. **Termination for Convenience (T4C) & Termination for Default (T4D)**
6. **Suspension and Debarment (FAR Subpart 9.4)**

Contract remedies may be severely limited if the contract fails to include appropriate language to address privacy and security issues. (Exception: *Christian doctrine*.)

According to one GAO report, almost half of contract actions it reviewed did not include such language.

Almost Half of Contract Actions Reviewed Lack Contract Provisions That Fully Safeguard Sensitive Information

For our analysis of contract documents for 42 contract actions at DHS, DOD, and HHS that involved contractor employees supporting mission-critical tasks, in order to be considered to fully safeguard all types of sensitive information, a contract had to contain provisions that specifically required contractors to refrain from (1) disclosing sensitive information to anyone except as needed for contract performance and (2) using such sensitive information for any purpose other than contract performance. In addition, the provisions had to cover the relevant types of sensitive information that may be accessed by a contractor during performance. As shown in table 3, our analysis found that slightly more than half of contract actions reviewed—23 of 42—contained contract provisions that fully safeguard the confidentiality and appropriate use of all types of sensitive information. In contrast, the remaining 19 contract actions reviewed did not extend safeguards to all relevant types of sensitive information that contractors may have had access to through the program offices they support. In the absence of such safeguards, there is higher risk of unauthorized disclosure or misuse of sensitive information by contractors.²⁸

²⁸Centers for Medicare and Medicaid Services (CMS), Acquisition Policy & Procedure Notice 12, Privacy Rule HIPAA Business Associate Contract Provision II (Baltimore, Md.: Apr. 21, 2006).

²⁹We did not consider the absence of such contract provisions as a deficiency unless they were also required by agency policy or the FAR.

II. FAR CLAUSES RELATING TO PRIVACY AND DATA SECURITY

OVERVIEW OF THE PRIVACY ACT OF 1974

2015 Edition



FAR Clauses: Privacy Act of 1974

- **Subsection (m) of the Privacy Act:** the Act applies to contractors operating a system of records by or for an agency to accomplish an agency function.
- **OMB Circular A-108 (Privacy Act guidance):** the Act extends to records collected or maintained by Federal contractors.

FAR Clauses: Privacy Act of 1974

- The contracting officer must insert **two Privacy Act clauses (FAR 52.224-1 and 52.224-2)** in the contract if **the contracting officer** determines that the contract requirements involve **the design, development, or operation** of a Privacy Act system.
- The contract work statement must **also identify the system of records (SOR)** and the relevant **design, development, or operation** work.
- The agency must provide its **“rules and regulations”** implementing the **Act** to the contractor.

FAR Clauses: Privacy Act of 1974

52.224-1 Privacy Act Notification.

Privacy Act Notification (Apr 1984)

The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

(End of clause)

FAR Clauses: Privacy Act of 1974

52.224-2 Privacy Act.

- **Privacy Act compliance, para. (a)(1):** The contractor agrees to comply with the Act and the agency's rules and regulations when the contract identifies the SOR and the design, development, or operation work that the contractor must perform.
- **Flowdown requirement, para. (a)(2):** The contractor agrees to include the Privacy Act notification clause in subcontracts and solicitations that require design, development, or operation of a SOR.
- **Liability, para. (b):** Contractor may be subject to civil and criminal penalties, and for purposes of the Privacy Act, the contractor shall be treated as an employee of the agency.
- **Definitions, para. (c):** "operation of a system of records"; "record"; and "system of records on individuals."

FAR Clauses: Privacy Act of 1974

TRUE OR FALSE?

The agency is responsible for identifying the “design, development, or operation” work to be performed by the contractor, the relevant SOR(s), and also for providing the contractor with the agency’s Privacy Act “rules and regulations.”

TRUE

FAR Clauses: Privacy Act of 1974

- The FAR Privacy Act clauses do not address many other Privacy Act responsibilities:
 - Establishing or modifying **system of records notices (SORNs)**
 - Providing **Privacy Act (e)(3) statements** when collecting information from individuals
 - Complying with **computer matching program** requirements
 - **Accounting for disclosures** of system records
 - Establishing appropriate **administrative, technical, and physical safeguards** (i.e., information security)

FAR Clause: IT Privacy or Security Safeguards

- **Privacy Act subsection (e)(10):** Agency must “establish appropriate **administrative, technical, and physical safeguards** to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.”
- **This clause applies when the contractor:**
 - is **designing, developing, or operating a SOR;** and
 - using **commercial IT services or IT support services.**

FAR Clause: IT Privacy or Security Safeguards

FAR 39.105 (instructions)

- Include agency rules of conduct with the contract
- List anticipated threats and hazards
- Specify the required safeguards
- Establish a Government inspection program

FAR 52.239-1 (clause)

- Contractor and Gov't must notify one another of new or unanticipated threats or hazards
- Contractor shall not disclose safeguards
- Contractor shall notify Government if safeguards cease to function
- Contractor shall provide access to its facilities (for inspections)

FAR Clause: Basic Safeguarding of Covered Contractor Information

- OMB Circular A-130, App. I-3-4: Agencies sharing PII with other entities shall impose conditions, **including security and privacy controls, through contracts** or other written agreement.
- For IT systems, the specific controls will depend on whether the contractor is using or operating a **Federal information system** or a **non-Federal information system**.

FAR Clause: Basic Safeguarding of Covered Contractor Information

FEDERAL

INFORMATION SYSTEMS

NIST SP 800-53,
rev. 5 (Sept. 2020,
rev. 12/10/2020)

Draft NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for
Information Systems and
Organizations

NON-FEDERAL

INFORMATION SYSTEMS

NIST SP 800-171, rev. 2
(Feb. 2020, updated
1/28/2021)

NIST Special Publication 800-171

Protecting Controlled Unclassified
Information in Nonfederal Information
Systems and Organizations

RON ROSS
PATRICK VISCUSO
GARY GUISSANIE
KELLEY DEMPSEY
MARK RIDDLE

A **federal information system** is a system used or operated by a contractor or other organization **on behalf of** an agency. See NIST SP 800-171, fn. 2. “On behalf of” means using or operating a system, or maintaining or collecting information, for the purpose of processing, storing, or transmitting Federal information, and such use, operation, maintenance, or collection is **not merely incidental** to providing goods or services to the Government. See NARA, Controlled Unclassified Information (CUI) Rule, 32 CFR 2002.4(hh).

Any other system is a **non-Federal information system**.

FAR Clause: Basic Safeguarding of Covered Contractor Information

- There is currently **no comprehensive FAR clause** that sets forth minimum **required security or privacy controls** for **Federal or non-Federal information systems** used or operated by contractors.
- NARA promised to sponsor a **new FAR clause for non-Federal information systems** under its Controlled Unclassified Information (CUI) Rule, 32 CFR part 2002, by 2017, to implement NIST SP 800-171 controls for those systems.
- In the meantime, see **FAR 4.1903** instructions and **FAR Clause 52.204-21**.

FAR Clause: Basic Safeguarding of Covered Contractor Information

Clause: FAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems (Jun 2016))

- Applies to any **“covered contractor information system”** that processes, stores or transmits **“Federal contractor information”** (i.e., **“information, not intended for public release, that is provided by or generated for the Government under a contract to deliver a product or service to the Government”**). This definition includes **nonpublic PII**.
- Excludes information provided to the public (e.g., websites) and “simple transactional information” (e.g., payment processing data).
- Requires **15 specific “measures or controls”** for “safeguarding” information systems.

FAR Clause: Basic Safeguarding of Covered Contractor Information

(b) Safeguarding requirements and procedures.

(1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

- (i) **Limit information system access to authorized users**, processes acting on behalf of authorized users, or devices (including other information systems).
- (ii) **Limit information system access to the types of transactions and functions** that **authorized users** are permitted to execute.
- (iii) Verify and control/limit connections to and use of **external information systems**.
- (iv) Control information posted or processed on **publicly accessible information systems**.
- (v) Identify **information system users**, processes acting on behalf of users, or devices.
- (vi) Authenticate (or verify) the identities of those users, processes, or devices, as a **prerequisite to allowing access** to organizational information systems.
- (vii) **Sanitize or destroy information system media** containing Federal Contract Information before disposal or release for reuse.

Grant
access only
to those
with a
need-to-know

Use records
only for
authorized
purposes

Identify individual
before granting
access to records

FAR Clause: Basic Safeguarding of Covered Contractor Information

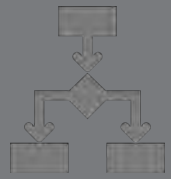


Establish appropriate physical safeguards

- (viii) **Limit physical access** to organizational information systems, equipment, and the respective operating environments to authorized individuals.
- (ix) **Escort visitors and monitor visitor activity**; maintain audit **logs of physical access**; and **control and manage physical access devices**.
- (x) Monitor, control, and protect **organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries** of the information systems.
- (xi) Implement subnetworks for **publicly accessible system components that are physically or logically separated from internal networks**.
- (xii) **Identify, report, and correct information** and information system flaws in a timely manner.
- (xiii) Provide protection from **malicious code** at appropriate locations within organizational information systems.
- (xiv) **Update malicious code protection mechanisms** when new releases are available.
- (xv) Perform **periodic scans of the information system** and real-time scans of files from external sources as files are downloaded, opened, or executed.

FAR Clause: Basic Safeguarding of Covered Contractor Information

- **Flowdown:** Must include the safeguards and this clause in **subcontracts** (including commercial items and items other than commercially available off-the-shelf) where PII or other nonpublic information covered by the clause is “**residing in or transiting through**” the subcontractor’s system.
- **Floor, not a ceiling:** Clause does not supersede **additional or other safeguarding requirements** that the contract may specify.



FAR Clause: Privacy Training

- OMB Circular A-130, App. I-11; NIST SP 800-53, rev. 5, AT-2 (AWARENESS TRAINING): “Provide **basic security and privacy awareness training** to system users (including managers, senior executives, and **contractors**)” as part of **initial training** for new users, when required by system changes and **at an organization-defined frequency** thereafter.

FAR Clause: Privacy Training

- **History**

- Proposed Rule, FAR Subpart 24.3 et al.—Privacy Training, 76 FR 63896 (Oct. 14, 2011)
- DHS Clause: Class Deviation 15-01 from the Homeland Security Acquisition Regulation: Safeguarding of Sensitive Information (March 9, 2015)
- **Final FAR Rule: Subpart 24.3, 81 FR 93480 (Dec. 20, 2016)**
- DHS Proposed Rules: 82 FR 6425 (privacy training), 6446 (IT security awareness training) (Jan. 19, 2017)

FAR Clause: Privacy Training

Instructions: see FAR 24.301 (Privacy training).

- Contractor must ensure their employees have **initial privacy training** and **annual privacy training** thereafter.
- These requirements apply to employees who have **access to a SOR**, who **design, develop, maintain, or operate a SOR**, or who otherwise **create, collect, use, process, store, maintain, disseminate, disclose, or otherwise “handle” PII** on the agency’s behalf.
- Training must be **role-based**; include **foundational and role-based training**; and **test users’ privacy knowledge**.

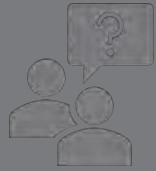
FAR Clause: Privacy Training

- At a minimum, training must cover—
 - (1) The provisions of the **Privacy Act of 1974 (5 U.S.C. 552a)**, including penalties for violations of the Act;
 - (2) The **appropriate handling and safeguarding** of personally identifiable information;
 - (3) The **authorized and official use** of a system of records or any other personally identifiable information;
 - (4) The restriction on the use of **unauthorized equipment** to create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise access personally identifiable information;
 - (5) The prohibition against the **unauthorized use of a system of records or unauthorized disclosure, access, handling, or use** of personally identifiable information; and
 - (6) Procedures to be followed in the event of a **suspected or confirmed breach** of a system of records or unauthorized disclosure, access, handling, or use of personally identifiable information (see Office of Management and Budget guidance for Preparing for and Responding to a Breach of Personally Identifiable Information).

FAR Clause: Privacy Training

- The contractor may **provide its own training or use the training of another agency** unless the contracting agency specifies that only its agency-provided training is acceptable (see 24.302(b)).
- The contractor is required to maintain and, upon request, to provide **documentation of completion of privacy training** for all applicable employees.
- No contractor employee shall be permitted to have or retain access to a system of records, create, collect, use, process, store, maintain, disseminate, disclose, or dispose, or otherwise handle personally identifiable information, or design, develop, maintain, or operate a system of records, **unless the employee has completed privacy training** that, at a minimum, addresses the elements in paragraph (b) of this section.





FAR Clause: Privacy Training

Clause: FAR 52.224-3 Privacy Training (Jan. 2017).

- Incorporates the OMB definition of PII
- Requires initial and annual private training
- Prescribes key elements of training
- Allows contractor to satisfy the training requirement by using agency-developed or -conducted training
- Requires contractor to maintain training documentation
- Prohibits access to PII by untrained employees
- Requirements must be flowed down to subcontractors handling PII
- Agency may require contractor to use only the agency's privacy training (see Alt. I)

FAR Clause: Privacy Training

TRUE OR FALSE?

All Federal contractors must use privacy training that is conducted or developed by the customer agency or the Federal Government.

FAR Clause: Rights in Data

- **Instructions:** FAR Subpart 27.4
- **Clauses:** FAR 52.227-14 et seq.
- **Purpose:** To define and balance the **Government's interest** in acquiring, accessing, and disseminating data under contract with the **contractor's proprietary interest** in such data.
- **"Data"** means recorded information, regardless of form or the media on which it may be recorded. The term includes technical data and computer software. The term does not include information incidental to contract administration, such as financial, administrative, cost or pricing, or management information. FAR 27.401 (definitions).





FAR Clause: Rights in Data

- 202. Ownership of **copyright** as distinct from ownership of **material object**
- Ownership of a copyright, or of any of the exclusive rights under a copyright, is distinct from ownership of any material object in which the work is embodied. Transfer of ownership of any material object, including the copy or phonorecord in which the work is first fixed, does not of itself convey any rights in the copyrighted work embodied in the object; nor, in the absence of an agreement, does transfer of ownership of a copyright or of any exclusive rights under a copyright convey property rights in any material object.
- Source: U.S. Copyright Office (Library of Congress), Circ. 92, "Copyright Law of the United States" (June 2020)

FAR Clause: Rights in Data

- **“Limited rights”** means the rights of the Government in limited rights data as set forth in a Limited Rights Notice.
 - **Software: “Restricted rights”** means the rights of the Government in restricted **computer software** as set forth in a Restricted Rights Notice.
- **“Unlimited rights”** means the rights of the Government to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose, and to have or permit others to do so.

FAR Clause: Rights in Data

True or false? When the Government's reserves "unlimited rights in data" first produced in the performance of the contract, a contractor still generally has a right to use, release to others, reproduce, such data or other data specifically used by the contractor in performing the contract.

- **True!** But the Contractor cannot use, release, reproduce, or publish such data where it is: (1) **prohibited by law or regulation;** (2) **expressly stated in the contract;** or (3) is contrary to **restrictive markings** placed on the data.

FAR Clause: Rights in Data

True or false? In general, a contractor may, without prior approval, assert copyright in **published scientific and technical articles** based on or containing data first produced in the performance of the contract.

- ❑ **True!** You may want, or be required by the Privacy Act of 1974, to limit or deny the Contractor's right to use Government's data in creating such articles, unless specifically approved by the Government.

FAR Clause: Kaspersky Labs (2018)

FAR Clause 52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities

- Prohibits contractors from:
 - **Providing** any hardware, software, or services developed or provided by **Russian-based Kaspersky Lab** or related entities; or
 - **Using** such hardware, software, or services in the development of data or deliverables first produced in the performance of the contract.
- Requires contractor to **report** any such hardware, software, or services discovered during contract performance.
- Requirements flow down to **subcontractors**.



FAR Clauses: Prohibited Telecom/Video Services & Equipment from China (2019)

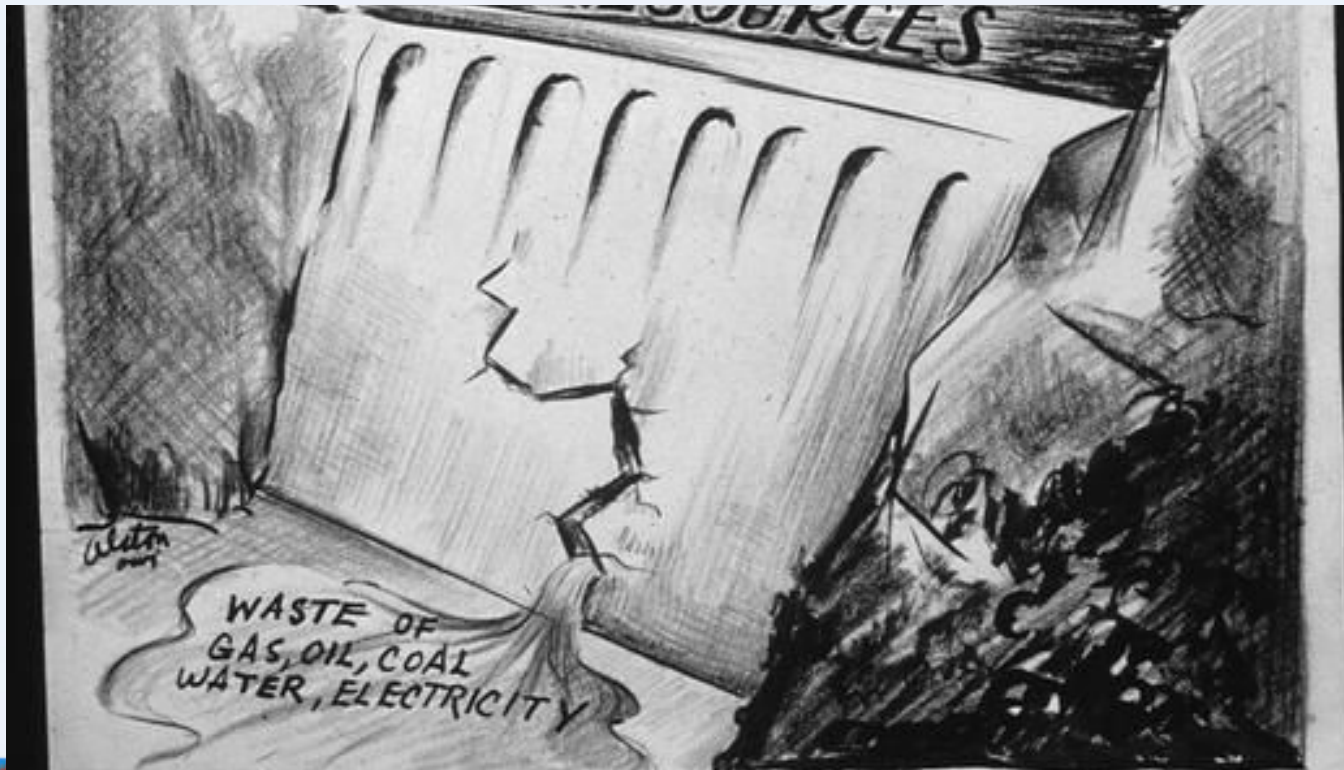
- Authority: sections **889(a)(1)(A) & (B)** of the NDAA for FY 2019 (Pub. L. 115-232).
- As a national security measure to protect Government information, and Government information and communication technology systems, agencies may not **(A)** procure any equipment, system, or service that uses **covered telecommunications equipment or services** as a substantial or essential component of any system, or as a critical technology as part of any system, or **(B) do business with any entity (prime contractor)** that uses such equipment, systems, or equipment from: **Huawei Technologies; ZTE Corp.; Hytera Communications; Hangzhou Hikvision; Dahua Technology; or an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country [People's Republic of China] as determined by the Sec'y of Defense.**
- **Interim Rule for sec. 889(a)(1)(A): FAR Case 2018-017**, 84 FR 40216 (Aug. 13, 2019), 84 FR 68314 (Dec. 13, 2019) (second interim rule), see also DoD and GSA implementing memos.
- **Interim Rule for sec. 889(a)(1)(B); FAR Case 2019-009**, submitted for publication to Federal Register (July 10, 2020, and eff. Aug. 13, 2020) ("The exfiltration of sensitive data from contractor systems arising from contractors' use of covered telecommunications equipment or services could also harm important governmental, **privacy**, and business interests.").

FAR Clauses: Prohibited Telecom/Video Services & Equipment from China (2019)

- **FAR Clause 52.204–24** requires offerors to represent **whether their offer includes covered telecommunications equipment or services** and if so, to **identify additional details** about its use. Alternatively, **FAR Clause 52.204-26** (annual certification in System for Awards Mgt. (SAM)).
- **FAR Clause 52.204–25** prohibits contractors from providing any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, **unless an exception applies or the covered telecommunications equipment or services are covered by a waiver described in FAR 4.2104.**
- The contractor must also **report** any such equipment, systems, or services **discovered during contract performance; this requirement flows down to subcontractors.**
- **See also GSAR 552.204-70 (for Federal Supply Schedule contracts)**

III. OTHER PRIVACY AND DATA SECURITY ISSUES IN FEDERAL CONTRACTS

Incident Response



Legal requirements:

- Privacy Act of 1974 (safeguards)
- OMB M-17-12 (Jan. 3, 2017)
- OMB Circular A-130, App. I-10

Incident Response

- **DFAR and HSAR Clauses**

- DFAR Revised Interim Rule (80 FR 81472, Dec. 30, 2015) for Safeguarding and Covered Defense Information Controls and Cyber Incident Reporting
- HSAR Class Deviation 15-01 from the Homeland Security Acquisition Regulation: Safeguarding of Sensitive Information (March 9, 2015)
- HSAR Case 2015-001: Safeguarding of Controlled Unclassified Information, 82 FR 6429 (Jan. 19, 2017) (proposed rule)—see paragraphs (d), (e) (incident response), (f) breach notification) (g) (credit monitoring)

Incident Response

- **Contractor must provide notice to the customer agency and/or US-CERT**
 - Notice needs to be timely, complete, and documented
- **Develop procedures for notifying and assisting affected individuals**
 - Who gives notice
 - Timing of notice (who decides, or is it automatic)
 - Contents of notice (who writes it, canned language, legal review)
 - Conflicting or overlapping state law notice obligations
 - Who answers questions from notified individuals
 - Will they need credit monitoring or other advice/assistance
 - Who pays for what

Incident Response

- Ensure the contractor will cooperate with **agency investigation and agency-directed mitigating measures**
 - Obtain access to logs, forensic analysis, other relevant contractor records (e.g., breach plan), facilities, employees
 - Impose or require sanctions (e.g., dismissing responsible individuals)
- Ensure that these requirements **flow down to subcontractors**

Incident Response

- **Outsource incident response tasks where appropriate and available**
 - GSA BPAs for Identity Protection Services (IPS)
 - To be replaced by SIN 520-20
 - E.g., credit monitoring and alerts
- **Adopt Privacy Act “routine use” in your SORNs**
 - Before you can share Privacy Act records (e.g., victims’ names and addresses from a system of records) with your contractor(s) or other agencies, you must have a **Privacy Act “routine use”** that authorizes such sharing/disclosure. **See OMB M-17-12 the for required text.**

Privacy Impact Assessment (PIA)

APPLICATION TO
IOT DEVICES



Privacy Impact Assessment (PIA)

Legal requirements

- E-GOV sec. 208
- IT Acquisitions and PRA Information Collection Activities– OMB 03-22
- Social Media – OMB 10-23

Privacy Impact Assessment (PIA)

- By definition, PIAs are required **before** you procure or have a contractor develop the technology or conduct a PRA information collection activity.
- Strive to assess privacy impact at the earliest possible stage of the acquisition planning process, as it may affect vendor options and technologies
 - PIAs are an explicit part of budgeting for Major IT Investments—OMB Exhibit A-300, but many purchases that require PIAs fall outside A-300
 - FedRAMP products (cloud services) do not come with a PIA

Privacy Impact Assessment (PIA)

- **Q: Will the following contracts involve “developing or procuring” “information technology” to “collect, maintain, or disseminate” PII?**
 - Contract for database services?
 - Contract for expert advisory/assistance services?
 - Contract for call center services?
 - Credit card purchase of electronic tablets?
 - Contractor’s service management interface where users must login?

Privacy Impact Assessment (PIA)

- Can the contractor do the PIA?
 - If the contractor is developing or provisioning a **Federal information system** (NIST SP 800-53), PIA may be incorporated into the process for assessing and authorizing the system to operate (ATO)
 - Contractors are generally unfamiliar with **some required elements** of a PIA (e.g., authority, types and uses of PII to be collected, maintained, or disseminated, whether the system is subject to the Privacy Act)
 - They may be in the best position to understand and **explain other PIA elements** (e.g., security controls, use of cookies or other tracking, data flows)
 - PIA is likely to be an **iterative, cooperative, and messy** process (e.g., agile software development may require an agile PIA)

Non-Disclosure Agreements (NDAs)

- Required by **Privacy Act**, **CUI Rule**, **NIST SP 800-53 & 800-171**
- **DFAR**
 - 252.204-7000 Disclosure of information
 - 252.204-7012 Safeguarding Covered Defense Information [includes CUI] and Cyber Incident Reporting
 - 252.204-7014 Limitations on the Use or Disclosure of Information by Litigation Support Contractors
- **HSAR**
 - 3052.204-71 Contractor employee access





Technical Documentation for Census Discs

Technical documentation for the Census Bureau American Housing Survey CD-ROM has been the topic of several questions recently received by GPO's Library Programs Service (LPS). This CD was distributed on shipping list 92-0003-E, dated March 20, 1992 (C 3.215/19:985-89/CD; item 0156-P). Users have questioned whether the hard copy technical documentation for this CD-ROM was distributed through the Federal Depository Library Program.

In most cases, according to Forrest Williams of the Census' Data User Services Division, the hard copy technical documentation which is sold by Census' Customer Services Office is exactly the same in content as the machine-readable technical documentation which is included on the disc. However, in a few cases, such as the American Housing Survey (AHS), the hard copy technical documentation is more detailed, and may include code lists for the data in addition to the record structure. Hard copy technical documentation for the AHS disc is reproduced internally as only 30 copies are needed for customers. Therefore the technical documentation is not printed through GPO and was not (and will not be) available to LPS for distribution to depository libraries. The technical documentation may be purchased from the Census Customer Services Office (301-763-4100) for \$10.00.

As was announced in Administrative Notes (v13-#4-2/15/92), LPS has reversed its earlier policy not to distribute hard copy technical documentation for electronic products when the technical documentation replicates information included on the disc. When such documentation is available to LPS it will be distributed to libraries.

There are two basic means by which LPS obtains paper documents for the depository program: 1) an agency requisitions a printing job through GPO, and LPS "rides" the requisition for copies; or 2) an agency has its publication printed outside of GPO and provides LPS with the number of copies needed for depository libraries. LPS will continue to work with the Census Bureau and other publishing agencies to ensure that the most complete documentation is distributed to depository libraries.

Depository librarians should also remember that microdata products, such as the AHS, require commercial statistical analysis software to be fully utilized. Such software is not available from either GPO or the Census Bureau.



Records Management

Legal Requirements:

- Federal Records Act
- NARA Guidance/Policies/Schedules
- OMB Circular A-130, p. 19 (records training for contractors)
- FAR 52.204-21 (requiring media data destruction or sanitization before disposal or re-use)

Records Management

- **Contractor records v. “agency records”**
 - *When do contractor records become “agency records”? FOIA test: see *Burka v. HHS*, 87 F.3d 508, 515 (D.C. Cir. 1996) (agency records include contractor records over which the agency exercised “**extensive supervision and control**,” citing *Tax Analysts v. Dep’t of Justice*, 845 F.2d 1060, 1069 (D.C. Cir. 1988), four-part “control” test*
 1. creator’s **intent**
 2. agency’s **use/disposal rights**
 3. agency’s **reading of or reliance** on records
 4. **integration** into agency files



Records Management

- See NARA Web site—*Model Records Management Language for Contracts*
 - Contractor must comply with Privacy Act of 1974 and safeguard records under the Act
 - “Federal records” include all records created for, delivered to, or under Government’s legal control
 - **All such records and rights therein are owned by U.S. Gov’t**
 - Prohibits unauthorized creation, retention, use, disclosure, removal, sale, destruction
 - Requires delivery, return, or destruction at Government’s direction
 - Use of Government-approved equipment only
 - Mandatory training
 - Subcontractor approval and flowdown of requirements

Records Management

Additional records management issues your contract should address:

- What will happen to contractor system **backups of PII**?
- How about **internal tracking and metadata** that may contain or reveal PII?
- Will the contractor provide a **certification of destruction** at contract close-out?
 - See HSAR Case 2015-001, 82 FR 6429 (Jan. 19, 2017) (proposed rule) at para. (h) (certificate of sanitization of Gov't and Gov't-activity-related files and information)
- **Will the Government's PII be segregated from other data?**
 - Should commingling be prohibited?
 - Should sensitive PII be stored separately?
- How will **legal process and other third-party requests** for the Government's PII be handled?

Web services/tracking

- Legal requirements:
 - E-GOV sec. 208 (privacy policy)
 - OMB M-10-22 (cookies et al.)
 - OMB M-10-23 (PIAs for social media)
 - Appropriations riders prohibit tracking of users across the Internet

Web services/tracking

- It's not always obvious when web services are part of a service contract—it may be buried or implicit in the SOW. *Ex.: benefits and claims administration, litigation expert services, records management.*
- Additional privacy risks of unauthorized marketing, advertising, or tracking—can you prohibit or have it blocked? *Ex.: social media or other commercial multi-tenant platforms.*

Privacy continuous monitoring

Relevant OMB Circular A-130 definitions:

- “37) ‘Information security continuous monitoring’ means maintaining ongoing awareness of information security, vulnerabilities, threats, and incidents to support agency risk management decisions.
- “58) ‘Privacy continuous monitoring’ means maintaining ongoing awareness of privacy risks and assessing privacy controls **at a frequency sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.”**

Privacy continuous monitoring

NIST SP 800-53, rev. 5, CA-7 (continuous monitoring for Federal information systems):

- The organization should develop a **system-level monitoring strategy** that establishes **metrics** and a **schedule for monitoring and assessing the effectiveness** of system controls.
- The organization should conduct **ongoing assessments** and should **monitor such metrics**, and should **correlate and analyze** the resulting information.
- The organization's strategy should also include **response actions** to address the results of its analyses, and **reporting of the security and privacy status** of the system to designated personnel or roles at a frequency defined by the organization.

Privacy continuous monitoring

HSAR (DHS) Case 2015-001, *supra*, 82 FR 6429, 6434 (Jan. 19, 2017) (proposed rule)

“(4) *Federal Reporting and **Continuous Monitoring Requirements***. Contractors operating information systems on behalf of the Government shall comply with Federal **reporting and information system continuous monitoring** requirements. * * * **Annual, quarterly, and monthly data collection will be coordinated by the Government.** The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for information systems. The Contractor shall provide the COR with requested information within three (3) business days of receipt of the request. Unless otherwise specified in the contract, **monthly continuous monitoring data shall be stored at the Contractor’s location for a period not less than one year from the date the data is created.** The Government may elect to perform **information system continuous monitoring** and IT security scanning of information systems from Government tools and infrastructure.”



FINAL GROUP EXERCISE

(see handout)

Resources

- Collected contract clauses from Federal agencies:
- <https://community.max.gov/display/Egov/Cybersecurity+In+Contracting+-+Agency+Practices>

Some critical lessons

- **Be involved as early as possible in the acquisitions process.**
 - That's why we have the PIA process.
 - Do not wait until solutions have been identified or procured.
 - Are you part of the long-term acquisitions planning process, not just contract-by-contract?

Some critical lessons

- **Get it in writing, and be specific as you can.**
 - OK: *Contractor shall comply with the Privacy Act of 1974.*
 - Better: *When collecting information from individuals, contractor shall provide the statement required by section (e)(3) of the Privacy Act of 1974. The contents of such statement shall be prescribed by the Government.*

Some critical lessons

- **You may need to ask the same question more than once.**
 - Are you asking the right person?
 - Even if you are, ask again and you may get a different or clearer answer.
 - Make sure you really know what PII your contractor is collecting, handling, creating, saving, sharing, and destroying, especially if the information is second-hand.

Contracting and privacy is a team effort.



- Public Affairs
- Human Capital Management/EEO
- Congressional Relations
- Records Management

Some critical lessons

- **You can't outsource your legal responsibility for privacy.**
 - The buck stops with the agency, not the contractor.



Questions?

- **Alex Tang, Assistant General Counsel, NSF**
 - 703-292-8547
 - ALTANG@nsf.gov
- **Thanks for attending!**

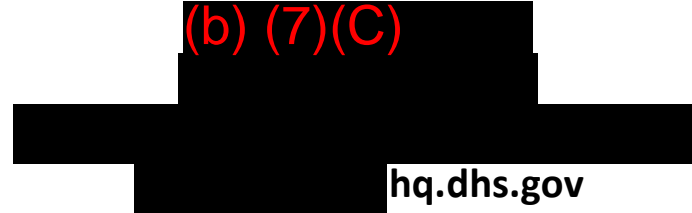


Federal **P**rivacy **C**ouncil

Federal Privacy Boot Camp

Session 7

(b) (7)(C)



Federal Privacy Council

Agenda

- Website Privacy Policies
- Privacy Principles for Mobile Applications
- Scanning Tools for Mobile Applications
- Privacy Compliance Process for Mobile Applications

Website Privacy Policies

- Section 208 of the E-Government Act requires agency website privacy policies to include the following information:
 - What information is collected through use of the website;
 - Why the information is being collected;
 - The intended use by the agency of the information;
 - With whom the information will be shared;
 - What notices or opportunities for consent will be provided;
 - How the information will be secured; and
 - The rights of individuals under the Privacy Act and other privacy laws.

Website Privacy Policies

- OMB M-03-22 (Sept. 2003) provides implementation guidance for agency website privacy policies
 - Requires agencies to post or provide links to their website privacy policies at their principal site and any web page that collects substantial information in an identifiable form
 - Website privacy policy must be clearly labeled, easily accessed, and written in plain language.
 - Requires agencies to provide a machine readable version of their website privacy policies that automatically lets a visitor know whether an agency's policy matches the visitor's privacy preferences

OMB M-17-06 (Nov. 2016)

- Requires that agencies post Privacy Policies on their principal, sub-agency, component, and program **websites, mobile applications**, and other digital services providing Privacy Act statements where required by the Privacy Act of 1974, and providing **privacy notices** for online collections of information where feasible.

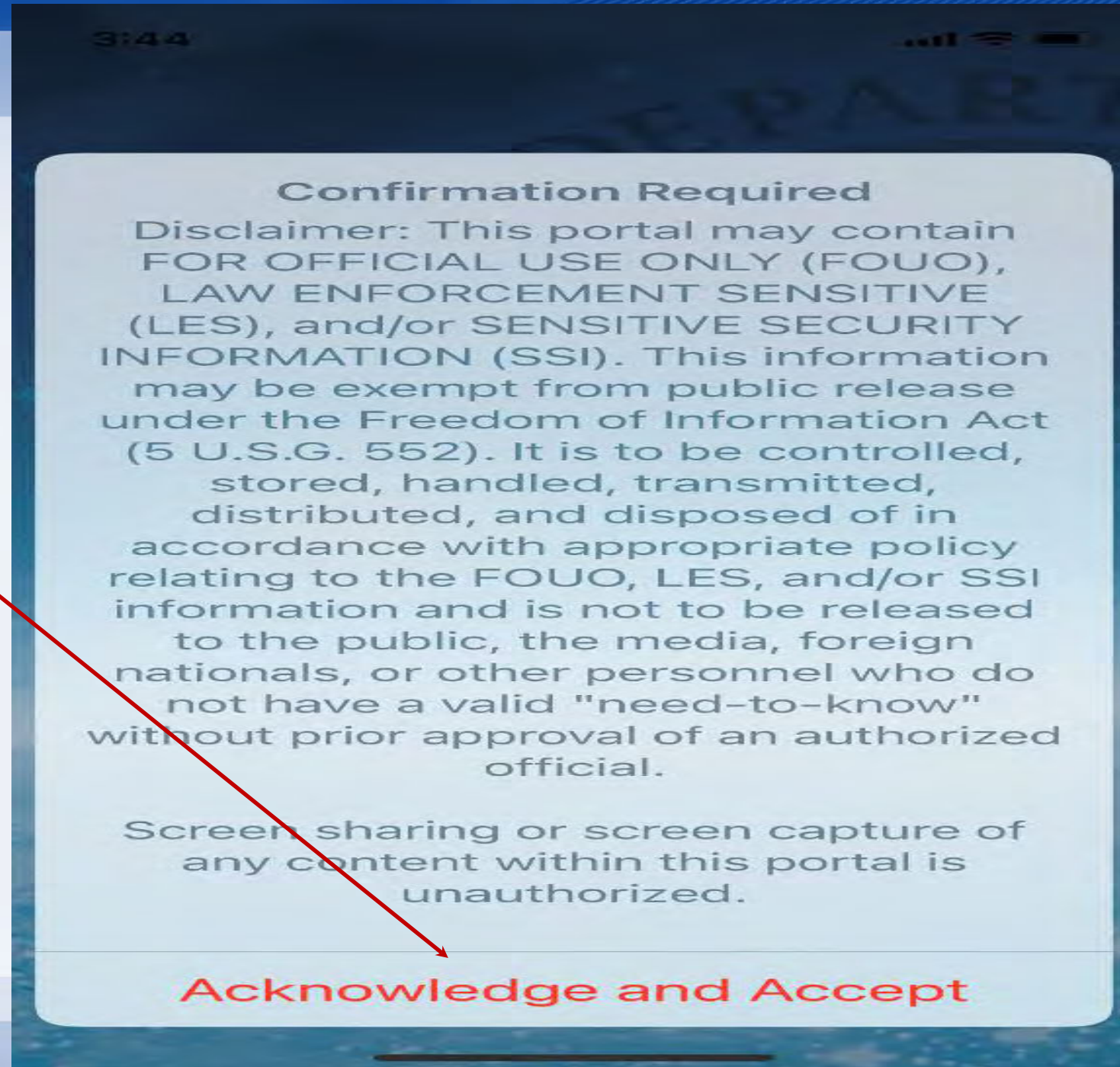
Privacy Principles for Mobile Applications

1. Provide Notice

- App-Specific Privacy Policy
- Privacy Statement
- Contextual Notice
 - Provided upon each update to the mobile app to specifically identify any changes to the uses of information from previous versions of the app;
 - Provided as “just-in-time” disclosures and obtain users’ affirmative express consent before a mobile app accesses sensitive content or other tools and applications on the mobile device for the first time (e.g., location services); and
 - Provided with independent opt-out features so that users may customize the mobile app’s features (e.g., opting out of location-based services, while still choosing to utilize other app services), where appropriate.

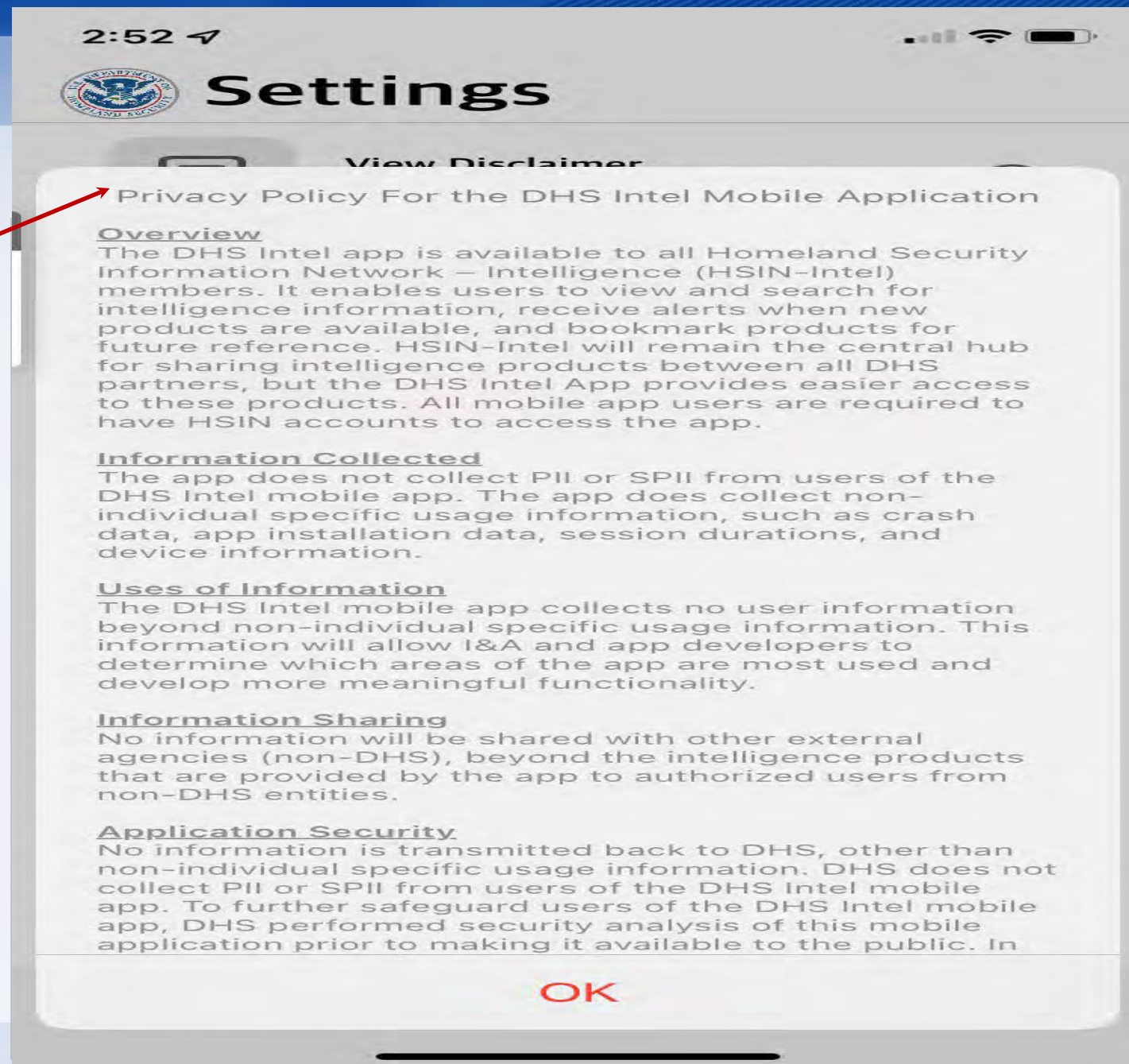
Example

Once users open the App users must choose to "Accept" before accessing the application



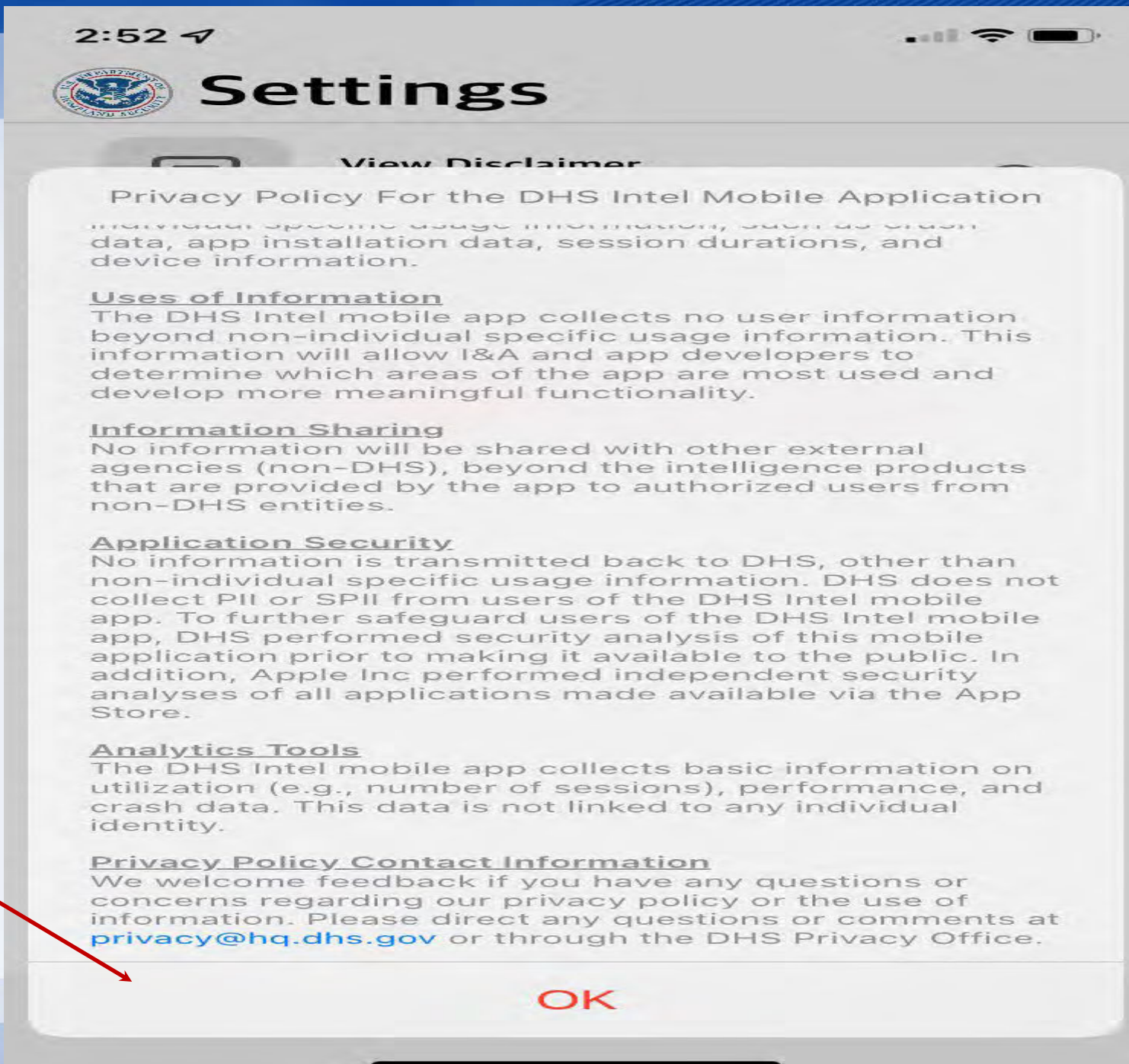
Example

When the App opens the Privacy Policy becomes available for review



Example

The user scrolls down the different provisions and then must concur



Example of App Collecting PII

Users tap the e(3) Privacy Act Statement when requested to provide PII. Users must choose to “Accept” before accessing the submission form.

Carrier 11:38 AM

Privacy Act

Privacy Act Statement
eFOIA Mobile Application

Authorities: 5 U.S.C. § 552, 5 U.S.C. § 552a, and 44 U.S.C. § 3101 authorize the collection of this information.

Purpose: DHS will use this information to locate applicable records and to respond to requests made under the Freedom of Information Act (5 U.S.C. § 552) and Privacy Act of 1974 (5 U.S.C. § 552a).

Routine Uses: This information may be used by and disclosed to DHS personnel, contractors, and/or other agents who need the information to assist in activities related to the processing of your Freedom of Information Act and/or Privacy Act request. Additionally, DHS may use the information, as necessary and authorized by the routine uses published in the DHS/ALL-001 - Department of Homeland Security (DHS) Freedom of Information Act (FIOA) and Privacy Act (PA) Record System February 4, 2014, 79 FR 6609.

Disclosure: Furnishing this information is voluntary; however, failure to provide the information requested may delay or prevent DHS from

Reject Accept

Privacy Principles for Mobile Applications

2. Limit the Collection and/or Use of Sensitive Content

- Mobile app features cannot collect and/or use PII, SPII, or other sensitive content unless directly needed to achieve an Agency's mission purpose.
- If the collection and/or use of PII, SPII, or sensitive content is directly necessary to achieve an Agency's mission purpose, then the collection and/or use of the information must be documented and justified in the mobile app's Privacy Compliance Documentation.

Privacy Principles for Mobile Applications

3. Establish Guidelines for User Submitted Information

- Where feasible, use forms and check boxes to limit data collection and minimize data entry errors.
- Provide a “review before sending” function that allows users to correct or opt-out of sending information.
- Unless necessary to achieve a mission purpose, limit ability of users to post information within the app that other users may view.
 - This will limit the potential for sharing PII, SPII, or other sensitive content unnecessarily.

Privacy Principles for Mobile Applications

4. Ensure Mobile App Security and Privacy

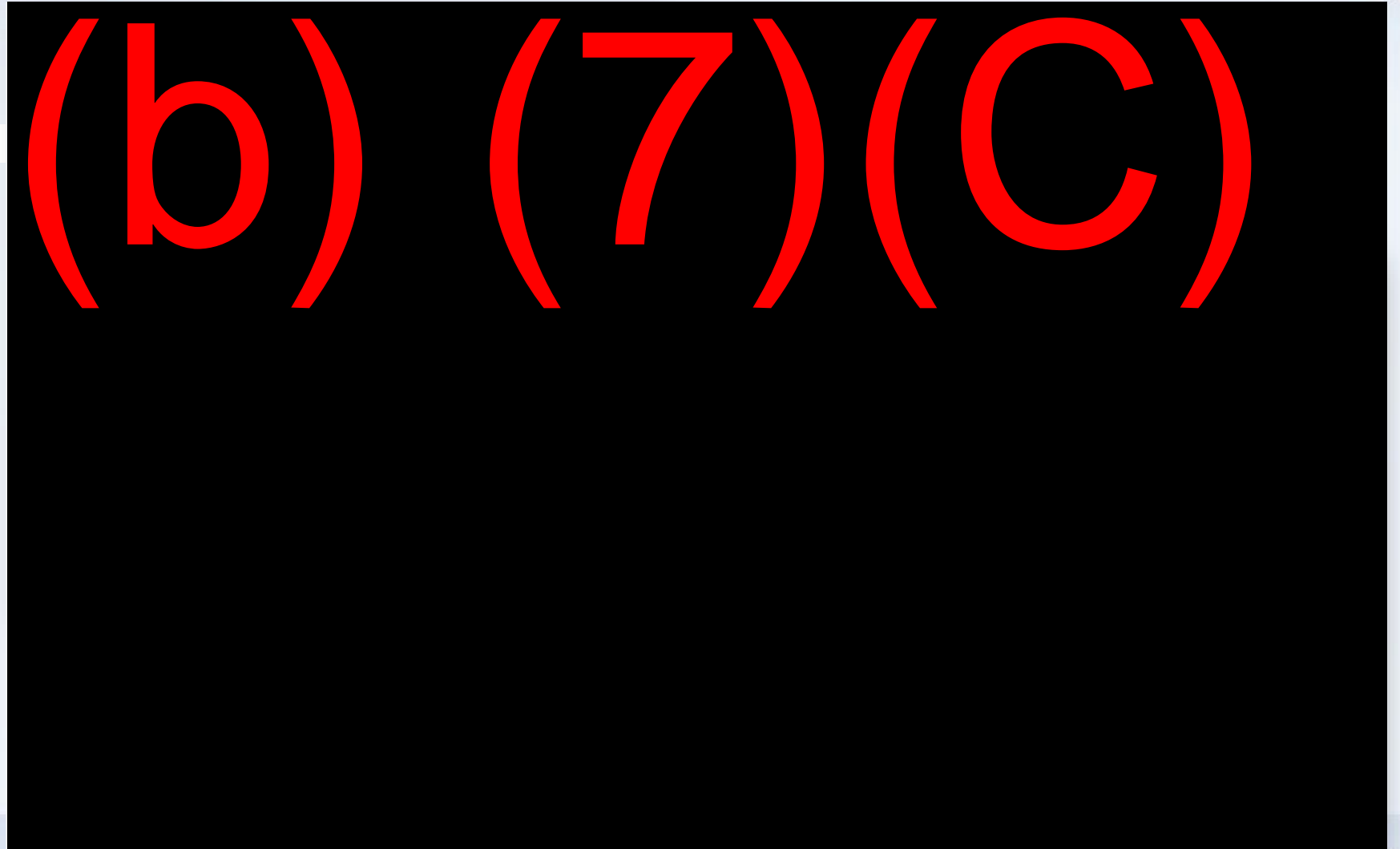
- Explore your Agency's ability to scan mobile apps for security and privacy vulnerabilities.
- If users submit sensitive information through your Agency's mobile app, that information should be encrypted in transit and immediately transferred to a protected internal Agency system that is compliant with your Agency's existing IT security policy;
- Sensitive content that a mobile app accesses or uses for the benefit of the user, but that your Agency does not need to collect (e.g., location information), should be locally stored within the mobile app or mobile device.

Mobile Application Assessment Tool

- The ability to utilize scanning tools that test for mobile app security and privacy vulnerabilities may be extremely helpful.
 - Can provide you with insight into what type of content the mobile app has access to (e.g., photos, videos, contacts, calendar, location-based services).
- Check with your Agency to see what options may currently exist.
 - If no such capabilities are currently available, you may contact the DHS OCIO Mobility Team (b) (7)(C) to see if the DHS Mobile Application Assessment Tool may work for you (iOS and Android applications only).

Mobile Application Assessment Tool Results

- A summary report is provided to tenants, with highlights of findings from multiple scanning tools



Mobile App Privacy Compliance Process

- Privacy compliance documentation should be completed for mobile apps in same manner as any new or updated system or project.
- If the ability to scan your mobile apps exists, then the results of those scans should be compared to the privacy compliance documentation to ensure that the documentation accurately describes the mobile app's collection, use, maintenance, retention, disclosure, deletion and destruction of PII, SPII, and other sensitive content. (ex. location services).



Federal Privacy Council